

A CATEGORICAL APPROACH TO PICARD-VESSIOT THEORY

ANDREAS MAURISCHAT

ABSTRACT. Picard-Vessiot rings are present in many settings like differential Galois theory, difference Galois theory and Galois theory of Artinian simple module algebras. In this article we set up an abstract framework in which we can prove theorems on existence and uniqueness of Picard-Vessiot rings, as well as on Galois groups corresponding to the Picard-Vessiot rings. As the present approach restricts to the categorical properties which all the categories of differential modules resp. difference modules etc. share, it gives unified proofs for all these Galois theories (and maybe more general ones).

1. INTRODUCTION

Since the foundation of Picard-Vessiot theory as a Galois theory for linear differential equations (cf. [20]), many analogues have evolved. For example, Picard-Vessiot theory for difference equations [23], for iterative differential equations [15], for C -ferential fields [22], for Artinian simple module algebras [2] and others.

In all these theories the base ring is a commutative ring with some operators acting on it, and the main objects are modules over that ring with the same operators acting.

The setting of Artinian simple module algebras generalises the setting of (iterative) differential fields as well as that of inversive difference pseudo-fields (i.e. simple difference rings which are a product of fields), but it does not generalise the difference setting where the given endomorphism is not bijective as in [26]. Y. André in [3] already gave a setting which unifies the case of difference pseudo-fields and differential fields in characteristic zero, however, it doesn't contain the Picard-Vessiot theory for differentially simple rings given in [18].

One could go further and generalise the operators even more or loosen the conditions on the base ring. However, there might still be cases not covered by such generalisations.

The present approach therefore restricts to the categorical properties which all the categories of differential modules resp. difference modules etc. share, and hence gives unified proofs for all these Picard-Vessiot theories (and more general ones).

The main results of this paper are the construction of a universal solution ring for a given “module” M such that all Picard-Vessiot rings (PV-rings) for M are quotients of this ring (Thm. 5.7 and Thm. 5.12), the existence of PV-rings

Date: July 16, 2015.

Key words and phrases. Tannakian categories, Picard-Vessiot theory, Galois theory.

up to a finite extension of constants (Thm. 5.18), and uniqueness of PV-rings inside a given simple solution ring with same constants (Prop. 5.14). Furthermore, we prove a correspondence between isomorphism classes of fibre functors $\omega : \langle\langle M \rangle\rangle \rightarrow \text{vect}_{\tilde{k}}$ and isomorphism classes of PV-rings R for $M \otimes_k \tilde{k}$, where k is the field of constants of the base ring S and \tilde{k} is any finite extension of k (Thm. 6.5). We also prove that the group scheme of automorphisms $\underline{\text{Aut}}^\partial(R/S)$ of R over S that commute with the extra structure, is isomorphic to the affine group scheme of automorphisms $\underline{\text{Aut}}^\otimes(\omega)$ of the corresponding fibre functor ω (Cor. 7.8). These two statements are direct generalisations of the corresponding facts given for example in [7, Ch. 9] or [3, Sect. 3.4 and 3.5].

Finally, we give a Galois correspondence between closed normal subgroup schemes of the Galois group scheme and subalgebras of the PV-ring which are PV-rings for some other “module”.

At this point we should mention that the setup of this article does not cover the parametrized Picard-Vessiot theories where the constants are equipped with an additional differential or difference operator as given for example in [6], [9], [11].

Differential setting. We now recall the main properties of the differential setting for having a better comparison with its analogs in the abstract setting. Classically, one starts with some differential field (F, ∂) of characteristic zero, and its field of differentially constant elements $k := F^\partial = \{x \in F \mid \partial(x) = 0\}$. The basic objects are differential modules (∂ -modules) (M, ∂_M) , i.e. F -vector spaces M with a derivation $\partial_M : M \rightarrow M$. Morphisms of ∂ -modules (called *differential homomorphisms*) are homomorphisms $f : M \rightarrow N$ of the underlying F -vector spaces which are compatible with the derivations, i.e. satisfy $f \circ \partial_M = \partial_N \circ f$. This implies that kernels and cokernels of ∂ -homomorphisms are again ∂ -modules, turning the category of ∂ -modules over (F, ∂) into an abelian category. For ∂ -modules (M, ∂_M) and (N, ∂_N) the tensor product $M \otimes_F N$ is naturally equipped with a derivation given by $\partial(m \otimes n) := \partial_M(m) \otimes n + m \otimes \partial_N(n)$. This provides the category of ∂ -modules with the structure of a symmetric monoidal category with unit object $\mathbb{1}$ given by the differential field (F, ∂) . Furthermore, for every ∂ -module (M, ∂_M) that is finitely generated as an F -vector space the dual vector space M^\vee carries a differential structure ∂_{M^\vee} such that the natural homomorphisms of evaluation $\text{ev} : M \otimes M^\vee \rightarrow F$ and coevaluation $\delta : F \rightarrow M^\vee \otimes M$ are ∂ -homomorphisms. This means that $(M^\vee, \partial_{M^\vee})$ is a dual of (M, ∂_M) in the category of ∂ -modules.

As we consider all ∂ -modules – and not only those which are finitely generated as F -vector spaces – this category is even closed under inductive limits. This is due to the fact that for a directed system $(M_i, \partial_i)_{i \in I}$ of differential modules, the inductive limit $\varinjlim_{i \in I} M_i$ of F -vector spaces can be equipped uniquely with a derivation compatible with the homomorphisms $M_i \rightarrow \varinjlim_{i \in I} M_i$.

The differential constants of a ∂ -module (M, ∂_M) are given as $M^\partial := \{m \in M \mid \partial_M(m) = 0\}$. This is a k -vector space of dimension at most $\dim_F(M)$. Therefore, one is interested in differential field extensions of F over which the corresponding dimensions are the same. From the view of linear differential

equations this means that the differential field extension contains a full set of solutions.

We assume now that the field of constants k is algebraically closed. A Picard-Vessiot extension of F for a ∂ -module (M, ∂_M) with $\dim_F(M) < \infty$ is defined to be a minimal differential field extension (E, ∂_E) of F such that $\dim_k((E \otimes_F M)^\partial) = \dim_E(E \otimes_F M) = \dim_F(M)$. A main theorem states that a Picard-Vessiot extension always exists and is unique up to differential isomorphism.

The differential Galois group $\text{Gal}(E/F)$ of a Picard-Vessiot extension E/F is then defined to be the group $\text{Aut}^\partial(E/F)$ of differential automorphisms of E fixing F . It has the structure of (k -rational points of) a linear algebraic group over k , and one obtains a Galois correspondence between the Zariski-closed subgroups of $\text{Gal}(E/F)$ and differential subfields of E containing F .

A main role is played by the Picard-Vessiot ring R in E . It is the subring of E which is generated as an F -algebra by the entries of a fundamental solution matrix and its inverse¹. R is a ∂ -simple ∂ -ring extension of F minimal with the property that $R \otimes_F M$ has a basis of constant elements. Here, ∂ -simple means that R has no nontrivial ideals stable under the derivation. Furthermore, E is the field of fractions of R , and $\text{Aut}^\partial(R/F) = \text{Aut}^\partial(E/F)$. Moreover, the spectrum $\text{Spec}(R)$ is a torsor of $\text{Gal}(E/F)$ over F . The Galois correspondence is more or less a consequence of this torsor property, as the subfield $E^\mathcal{H}$ corresponding to a closed subgroup $\mathcal{H} \leq \text{Gal}(E/F)$ is nothing else than the field of rational functions on the scheme $\text{Spec}(R)/\mathcal{H}$.

If the field of constants k is not algebraically closed (cf. [10] and [16]), some things become more involved. First at all, one also requires that a Picard-Vessiot field E has the same field of constants k – a condition which is automatically fulfilled if k is algebraically closed. Furthermore, the Galois group has to be replaced by a representable group functor $\underline{\text{Gal}}(E/F)$, i.e. an affine group scheme, whose group of k -rational points is $\text{Aut}^\partial(E/F)$. Then as above, $\text{Spec}(R)$ is a $\underline{\text{Gal}}(E/F)$ -torsor over F and one obtains a Galois correspondence between closed subgroups of $\underline{\text{Gal}}(E/F)$ and differential subfields of E containing F . However, since the constants are not algebraically closed, existence of a Picard-Vessiot field or a Picard-Vessiot ring is not guaranteed, and also uniqueness might fail. Furthermore, assume one is given a PV-field E , the Galois group scheme does not act algebraically on the PV-field but only on the PV-ring. On the other hand, one does not get a full Galois correspondence on the ring level. The geometric reason is that for a closed subgroup $\mathcal{H} \leq \underline{\text{Gal}}(E/F)$ the invariant ring $R^\mathcal{H}$ is the ring of global sections of the orbit space $\text{Spec}(R)/\mathcal{H}$. If the latter is not affine, $R^\mathcal{H}$ becomes “too small”.

On the ring level, at least one has a restricted Galois correspondence between closed normal subgroups of $\underline{\text{Gal}}(E/F)$ and differential subrings of R containing F which are Picard-Vessiot rings for some ∂ -module (cf. [18]).

In the abstract setting of this article, we will stay on the ring level, since the action of the Galois group is naturally algebraic there.

¹A fundamental solution matrix is a base change matrix over E mapping an F -basis of M to a k -basis of $(E \otimes_F M)^\partial$, both bases seen as E -bases of $E \otimes_F M$.

Iterative differential and difference setting. In iterative differential Galois theory in arbitrary characteristic derivations are replaced by so called iterative derivations (cf. [15]). These are a collection $\theta = (\theta^{(n)})_{n \in \mathbb{N}}$ of additive maps satisfying $\theta^{(0)} = \text{id}$, $\theta^{(n)}(ab) = \sum_{i+j=n} \theta^{(i)}(a)\theta^{(j)}(b)$ as well as $\theta^{(n+m)} = \binom{n+m}{n} \theta^{(n)} \circ \theta^{(m)}$ for all $n, m \in \mathbb{N}$. This means, $\partial := \theta^{(1)}$ is a derivation and $\theta^{(n)}$ resembles $\frac{1}{n!} \partial^n$ – the n -th iterate of ∂ divided by n -factorial. Indeed, in characteristic zero, the iterative derivations are determined by the derivation $\partial = \theta^{(1)}$ via $\theta^{(n)} = \frac{1}{n!} \partial^n$. In particular the differential setting in characteristic zero is a special case of the iterative differential setting. The constants of an iterative differential field (F, θ) are given by $F^\theta := \{x \in F \mid \theta^{(n)}(x) = 0 \forall n \geq 1\}$. The basic objects are iterative differential modules (M, θ_M) , and one is interested in minimal iterative differential extensions E of F (with same constants) such that $\dim_{F^\theta} ((E \otimes_F M)^\theta) = \dim_F(M)$. All the things about Picard-Vessiot rings and fields turn out the same as in the differential setting. However, even in the case that $k = F^\theta$ is algebraically closed, one has to consider the Galois group as an affine group scheme which might be nonreduced (if E/F is not separable) (cf. [17], [16]).

In difference Galois theory derivations are replaced by automorphisms and constants by invariants, i.e. one starts with some field F together with an automorphism $\sigma : F \rightarrow F$ and its field of invariant elements $k := F^\sigma := \{x \in F \mid \sigma(x) = x\}$. The basic objects are difference modules (M, σ_M) , i.e. F -vector spaces M together with a σ -linear automorphism $\sigma_M : M \rightarrow M$. Again, the set of invariants $M^\sigma := \{m \in M \mid \sigma_M(m) = m\}$ is a k -vector space of dimension at most $\dim_F(M)$, and one is interested in a difference extension of F over which the corresponding dimensions are the same. In this setting another aspect appears, since in some situations every solution ring has zerodivisors. Hence even if k is algebraically closed, there does not exist a Picard-Vessiot **field** in general. Nevertheless, if k is algebraically closed, there always exists a Picard-Vessiot ring R over F , i.e. a σ -simple σ -ring extension R of F minimal with the property that $R \otimes_F M$ has a basis of invariant elements, and instead of the Picard-Vessiot field one considers $E = \text{Frac}(R)$, the total ring of fractions of R . With these definitions one again obtains a Galois group scheme $\underline{\text{Gal}}(R/F)$ as a representable functor whose k -rational points are exactly $\text{Aut}^\sigma(R/F) = \text{Aut}^\sigma(E/F)$, as well as a Galois correspondence between closed subgroup schemes of $\underline{\text{Gal}}(R/F)$ and total difference subrings of E containing F .

Other settings. The three basic settings described above have been generalised in various ways. First at all, the operators acting have become more general: Takeuchi in [22] considered an action of a pointed irreducible cocommutative coalgebra C on the base field F (which he then calls a C -ferential field). This amounts to having a collection of several commuting higher derivations. Later Amano-Masuoka in [2] have considered an action of a pointed cocommutative Hopf-algebra D on the base field F (then called D -module algebra), though generalising to a collection of commuting iterative derivations and automorphisms. André in [3] used so called noncommutative differentials in characteristic 0 resembling a collection of derivations and endomorphisms.

On the other hand, also the bases have become more general: the base field F has been generalised to (i) an Artinian algebra (i.e. finite product of fields) which is simple as D -module algebra in [2], (ii) a Noetherian ring which is simple with respect to the differentials in [3], and (iii) any differentially simple (iterative) differential ring in [18].

In [12, Ch. 2], N. Katz even considers schemes \mathcal{X} of finite type over k , and obtains Picard-Vessiot extensions for finitely generated $\mathcal{O}_{\mathcal{X}}$ -modules with integrable connections.

All these settings have in common that you start with a base ring (or even base scheme) F with some extra structure such that no non-trivial ideal of F is respected by the extra structure, i.e. that F is simple. The basic objects for which one considers Picard-Vessiot rings are finitely generated modules over F with corresponding extra structure having a dual in the category of modules with extra structure, and the Picard-Vessiot rings are algebra objects in the category of (all) modules with extra structure.

Abstract setting. In the abstract setting this is reflected by the following basic setup:

- (C1) \mathcal{C} is an abelian symmetric monoidal category with unit object $\mathbb{1} \in \mathcal{C}$.
We assume that $\mathbb{1}$ is a simple object in \mathcal{C} .
- (C2) \mathcal{C} is cocomplete, i.e. \mathcal{C} is closed under small inductive limits.
- (F1) There is a scheme \mathcal{X} , and an additive tensor functor $v : \mathcal{C} \rightarrow \mathbf{Qcoh}(\mathcal{X})$ from \mathcal{C} to the category of quasi-coherent $\mathcal{O}_{\mathcal{X}}$ -modules which is faithful, exact and preserves small inductive limits. (In particular, $v(\mathbb{1}) = \mathcal{O}_{\mathcal{X}}$.)
- (F2) $M \in \mathcal{C}$ is dualizable whenever $v(M)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$ -module.

It is this basic setup from which all the statements on Picard-Vessiot rings and their Galois groups follow. For stating those, one has to transfer several concepts into the abstract setting; most important the concept of constants/invariants: It is not hard to see that for every differential module (M, ∂_M) over F the constants M^∂ of M can also be given as the vector space $\mathrm{Hom}_F^\partial(F, M)$ of differential homomorphisms $f : F \rightarrow M$, since every F -homomorphism $f : F \rightarrow M$ is uniquely determined by the image of $1 \in F^\partial \subseteq F$. Similarly, the invariants M^σ of a difference module (M, σ_M) can be given as $\mathrm{Hom}_F^\sigma(F, M)$. Hence, in the abstract setting, “taking constants” is given by the functor $()^\mathcal{C} := \mathrm{Mor}_{\mathcal{C}}(\mathbb{1}, -) : \mathcal{C} \rightarrow \mathbf{Vect}_k$ where k is the field $k = \mathrm{End}_{\mathcal{C}}(\mathbb{1})$ corresponding to the constants of a differential field F resp. the invariants of a difference field F .

The condition on a Picard-Vessiot ring R for M that the module $R \otimes_F M$ has a basis of constants/invariants is given abstractly by the condition that the natural morphism $\varepsilon_{R \otimes M} : R \otimes \iota((R \otimes M)^\mathcal{C}) \rightarrow R \otimes M$ is an isomorphism in the category \mathcal{C} (cf. Prop. 4.6). Here $\iota : \mathbf{Vect}_k \rightarrow \mathcal{C}$ is a functor corresponding to the construction of a differential/difference module out of a F^∂ -vector space by tensoring with the base differential/difference ring F .

The article is structured as follows. In Section 2, we prove a theorem on commutative algebras which will later be used for showing that the constants of minimal simple solution rings are just a finite extension of the constants k ,

and in particular guarantee the existence of Picard-Vessiot rings up to a finite extension of constants.

In Section 3, we investigate some properties of the functors $()^{\mathcal{C}}$ and ι . In particular, we show that the functor $()^{\mathcal{C}}$ is right adjoint to ι . Furthermore, we show that the unit $\eta : \text{id}_{\text{Vect}_k} \rightarrow ()^{\mathcal{C}} \circ \iota$ of the adjunction is a natural isomorphism, and that the counit $\varepsilon : \iota \circ ()^{\mathcal{C}} \rightarrow \text{id}_{\mathcal{C}}$ of the adjunction provides a monomorphism ε_M for every $M \in \mathcal{C}$. The latter corresponds to the fact in the differential setting that the natural homomorphism $F \otimes_k M^{\partial} \rightarrow M$ is injective. Section 4 is dedicated to commutative algebras R in the category \mathcal{C} and the category \mathcal{C}_R of R -modules in \mathcal{C} as given in [13], as well as properties of the functors ι_R and $()^{\mathcal{C}_R}$ similar to those of ι and $()^{\mathcal{C}}$, under certain assumptions on the algebra R .

Solution rings and Picard-Vessiot rings are then the subject of Section 5, where also the theorems on existence and uniqueness of Picard-Vessiot rings are proven. The objective of Section 6 is the correspondence between isomorphism classes of Picard-Vessiot rings for a given dualizable $M \in \mathcal{C}$ and isomorphism classes of fibre functors from the strictly full abelian tensor subcategory $\langle\langle M \rangle\rangle$ of \mathcal{C} to Vect_k .

In Section 7 we consider the group functors $\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R)$ of automorphisms of R and $\underline{\text{Aut}}^{\otimes}(\omega_R)$ of automorphisms of the corresponding fibre functor ω_R , and we show that they are both isomorphic to the spectrum of the k -algebra $\omega_R(R) = (R \otimes R)^{\mathcal{C}}$. As the latter will be proven to be a Hopf-algebra of finite type over k , both group functors are indeed affine group schemes of finite type over k .

Finally, in Section 8 we prove the Galois correspondence between normal closed subgroups of the Galois group scheme $\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R)$ and \mathcal{C} -subalgebras of R that are Picard-Vessiot rings for some dualizable $N \in \mathcal{C}$.

Acknowledgements. I would like to thank G. Böckle and F. Heiderich for their comments on earlier versions which helped a lot to improve the paper. I would also like to thank M. Wibmer, as only a common project with him drew my attention to this general abstract setting.

2. A COMMUTATIVE ALGEBRA THEOREM

We will be faced with the question whether there exists a Picard-Vessiot ring up to a finite extension of constants. The following theorem will be a key ingredient to the existence proof. All algebras are assumed to be commutative with unit.

Theorem 2.1. *Let k be a field, S an algebra over k and R a finitely generated flat S -algebra. Furthermore, let ℓ be a field extension of k such that $S \otimes_k \ell$ embeds into R as an S -algebra. Then ℓ is a finite extension of k .*

Proof. The proof is split in several steps:

1) Reduction to S being a field

Choose a minimal prime ideal \mathfrak{p} of S , and let $S_{\mathfrak{p}}$ denote the localization of S at \mathfrak{p} . Since localizations are flat, the inclusion of rings $S \subseteq S \otimes_k \ell \subseteq R$ induces an inclusion of rings

$$S_{\mathfrak{p}} \subseteq S_{\mathfrak{p}} \otimes_k \ell \subseteq S_{\mathfrak{p}} \otimes_S R,$$

and $S_{\mathfrak{p}} \otimes_S R$ is a finitely generated $S_{\mathfrak{p}}$ -algebra. Since flatness is stable under base change, $S_{\mathfrak{p}} \otimes_S R$ is a flat $S_{\mathfrak{p}}$ -algebra.

Since $\mathfrak{p}S_{\mathfrak{p}}$ is the maximal ideal of $S_{\mathfrak{p}}$, $\bar{S} := S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ is a field, and $\bar{R} := S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}} \otimes_S R$ is a finitely generated flat algebra over \bar{S} . It remains to show that $\bar{S} \otimes_k \ell$ embeds into \bar{R} .

Since $S_{\mathfrak{p}} \otimes_k \ell$ and $S_{\mathfrak{p}} \otimes_S R$ are both flat over $S_{\mathfrak{p}}$, the exact sequence $0 \rightarrow \mathfrak{p}S_{\mathfrak{p}} \rightarrow S_{\mathfrak{p}} \rightarrow S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}} \rightarrow 0$ leads to a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathfrak{p}S_{\mathfrak{p}} \otimes_k \ell & \longrightarrow & S_{\mathfrak{p}} \otimes_k \ell & \longrightarrow & (S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}) \otimes_k \ell \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathfrak{p}S_{\mathfrak{p}} \otimes_S R & \longrightarrow & S_{\mathfrak{p}} \otimes_S R & \longrightarrow & (S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}) \otimes_S R \longrightarrow 0. \end{array}$$

Then the last vertical arrow is an injection if the left square is a pullback diagram. Hence, we have to proof that any element in $S_{\mathfrak{p}} \otimes_k \ell$ whose image in $S_{\mathfrak{p}} \otimes_S R$ actually lies in $\mathfrak{p}S_{\mathfrak{p}} \otimes_S R$ is an element of $\mathfrak{p}S_{\mathfrak{p}} \otimes_k \ell$.

Hence, let $z = \sum_{i=1}^n s_i \otimes x_i \in S_{\mathfrak{p}} \otimes_k \ell$ with k -linearly independent $x_1, \dots, x_n \in \ell$, and let $w = \sum_{j=1}^m a_j \otimes r_j \in \mathfrak{p}S_{\mathfrak{p}} \otimes_S R$ such that their images in $S_{\mathfrak{p}} \otimes_S R$ are the same. Since all elements in $\mathfrak{p}S_{\mathfrak{p}}$ are nilpotent, there is $e_1 \geq 0$ maximal such that $a_1^{e_1} \neq 0$. Inductively for $j = 2, \dots, m$, there is $e_j \geq 0$ maximal such that $a_1^{e_1} \cdots a_j^{e_j} \neq 0$. Let $a := \prod_{j=1}^m a_j^{e_j} \in S_{\mathfrak{p}}$. Then by construction, $a \neq 0$ but $a \cdot w = \sum_{j=1}^m a a_j \otimes r_j = 0$. So $0 = a \cdot z = \sum_{i=1}^n a s_i \otimes x_i$, i.e. $a s_i = 0$ for all i . Since $a \neq 0$, one obtains $s_i \notin (S_{\mathfrak{p}})^{\times}$, i.e. $s_i \in \mathfrak{p}S_{\mathfrak{p}}$.

From now on, we may and will assume that S is a field. In this case R is Noetherian as it is a finitely generated S -algebra.

2) Proof that ℓ is algebraic over k

Assume that ℓ is not algebraic over k , then there is an element $a \in \ell$ transcendental over k . By assumption, a is also transcendental over S inside R , i.e. the polynomial ring $S[a]$ is a subring of R . The image of the corresponding morphism $\psi : \text{Spec}(R) \rightarrow \text{Spec}(S[a]) \cong \mathbb{A}_S^1$ is a dense subset of $\text{Spec}(S[a])$, since the ringhomomorphism is an inclusion, and it is locally closed by [4, Cor. 3, Ch. V, §3.1]. Hence, the image is open. But for all $0 \neq f \in k[a]$, the irreducible factors of f in $S[a]$, are invertible in $\ell \subseteq R$. Hence, infinitely many maximal ideals of $\text{Spec}(S[a])$ are not in the image of ψ – contradicting that the image is open.

3) Proof that ℓ is finite over k

For showing that ℓ is indeed finite over k , we give a bound on $[\ell' : k]$ for any $\ell' \subseteq \ell$ which is finite over k , and this bound only depends on data of R . Since ℓ is the union of all its finite subextensions this proves finiteness of ℓ .

For simplicity we again write ℓ for the finite extension ℓ' of k .

Let

$$(0) = \bigcap_{i=1}^c \mathfrak{q}_i$$

be a primary decomposition of the zero ideal $(0) \subseteq R$ and $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ the corresponding prime ideals. Furthermore, let $N_i \in \mathbb{N}$ satisfy $\mathfrak{p}_i^{N_i} \subseteq \mathfrak{q}_i$, i.e. for all

$y_1, \dots, y_{N_i} \in \mathfrak{p}_i$, one has $y_1 \cdot y_2 \cdots y_{N_i} \in \mathfrak{q}_i$.² Furthermore, for each $i = 1, \dots, c$ let $\mathfrak{m}_i \subseteq R$ be a maximal ideal containing \mathfrak{p}_i . Then $d_i := \dim_S R/\mathfrak{m}_i$ is finite for all i .

We claim that $\dim_k(\ell)$ is bounded by $2 \cdot \sum_{i=1}^c d_i \cdot N_i$:

First at all $R \rightarrow \prod_{i=1}^c R/\mathfrak{q}_i$ is an injective S -algebra homomorphism and R/\mathfrak{q}_i is irreducible with unique minimal ideal \mathfrak{p}_i .

Letting $\tilde{\mathfrak{q}}_i := \mathfrak{q}_i \cap (S \otimes_k \ell)$, and $\tilde{\mathfrak{p}}_i := \mathfrak{p}_i \cap (S \otimes_k \ell) = \sqrt{\tilde{\mathfrak{q}}_i}$, then $(S \otimes_k \ell)/\tilde{\mathfrak{q}}_i$ embeds into R/\mathfrak{q}_i , and $S \otimes_k \ell \rightarrow \prod_{i=1}^c (S \otimes_k \ell)/\tilde{\mathfrak{q}}_i$ is injective. It therefore suffices to show that $\dim_S((S \otimes_k \ell)/\tilde{\mathfrak{q}}_i) \leq 2d_i N_i$ holds for each i . In the following we therefore consider an arbitrary component and will omit the index i .

Since $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is a finite S -algebra, and $\tilde{\mathfrak{p}}$ is its unique minimal prime ideal, $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is a local Artinian algebra with residue field $(S \otimes_k \ell)/\tilde{\mathfrak{p}}$. Since $(S \otimes_k \ell)/\tilde{\mathfrak{p}}$ is a field, the composition

$$(S \otimes_k \ell)/\tilde{\mathfrak{p}} \hookrightarrow R/\mathfrak{p} \rightarrow R/\mathfrak{m}$$

is injective. Hence,

$$\dim_S((S \otimes_k \ell)/\tilde{\mathfrak{p}}) \leq \dim_S(R/\mathfrak{m}) = d.$$

It remains to show that $\dim_{(S \otimes_k \ell)/\tilde{\mathfrak{p}}}((S \otimes_k \ell)/\tilde{\mathfrak{q}}) \leq 2N$.

As a tensor product of fields and as ℓ/k is finite, $S \otimes_k \ell$ is a finite direct product of local artinian algebras with residue fields being finite extensions of S . The local algebra over some finite extension S' of S is given as $S' \otimes_{k'} \tilde{k}$ for a finite extension k' of k contained in S' and a purely inseparable extension \tilde{k}/k' .

In particular, also the algebra $(S \otimes_k \ell)/\tilde{\mathfrak{q}}$ is of that form (as it is just isomorphic to one factor of $(S \otimes_k \ell)$). Hence, let S' , k' and \tilde{k} be such that $(S \otimes_k \ell)/\tilde{\mathfrak{p}} \cong S'$ and $(S \otimes_k \ell)/\tilde{\mathfrak{q}} \cong S' \otimes_{k'} \tilde{k}$. As \tilde{k} is purely inseparable over k' , there are $x_1, \dots, x_t \in \tilde{k}$, $m_1, \dots, m_t \in \mathbb{N}$ and $a_1, \dots, a_t \in k'$ such that

$$\tilde{k} = k'[x_1, \dots, x_t] / (x_1^{p^{m_1}} - a_1, \dots, x_t^{p^{m_t}} - a_t).$$

where p denotes the characteristic of the fields. As $S' \otimes_{k'} \tilde{k}$ is local with residue field S' , there are also $s_1, \dots, s_t \in S'$ such that $s_j^{p^{m_j}} = a_j$ for all $j = 1, \dots, t$, and $S' \otimes_{k'} \tilde{k}$ is given as

$$S' \otimes_{k'} \tilde{k} \cong S'[x_1, \dots, x_t] / ((x_1 - s_1)^{p^{m_1}}, \dots, (x_t - s_t)^{p^{m_t}}).$$

In particular its nilradical (corresponding to $\tilde{\mathfrak{p}}$) is generated by $(x_1 - s_1, \dots, x_t - s_t)$.

Since $\tilde{\mathfrak{p}}^N \subseteq \tilde{\mathfrak{q}}$, and $(x_1 - s_1)^{p^{m_1}-1} \cdots (x_t - s_t)^{p^{m_t}-1} \neq 0$ we obtain that

$$N > \sum_{j=1}^t (p^{m_j} - 1) \geq \sum_{j=1}^t \frac{1}{2} p^{m_j} = \frac{1}{2} \dim_{S'}(S' \otimes_{k'} \tilde{k}).$$

Therefore, we have shown that $\dim_{(S \otimes_k \ell)/\tilde{\mathfrak{p}}}((S \otimes_k \ell)/\tilde{\mathfrak{q}}) < 2N$.

□

²This N_i exists since R is Noetherian and therefore \mathfrak{p}_i is finitely generated.

3. SETUP AND BASIC PROPERTIES

In this section, we set up an abstract framework in which we can prove theorems on Picard-Vessiot extensions, as well as their Galois groups. The theorems thus apply to all kinds of differential and difference Galois theories which match the basic setup given below. The setup therefore provides a uniform approach to the existing theories.

We consider the following setup:

- (C1) \mathcal{C} is a locally small abelian symmetric monoidal category with unit object $\mathbb{1} \in \mathcal{C}$. We assume that $\mathbb{1}$ is a simple object in \mathcal{C} .
- (C2) \mathcal{C} is cocomplete, i.e. \mathcal{C} is closed under small inductive limits.
- (F1) There is a scheme \mathcal{X} , and an additive tensor functor $v : \mathcal{C} \rightarrow \mathbf{Qcoh}(\mathcal{X})$ from \mathcal{C} to the category of quasi-coherent $\mathcal{O}_{\mathcal{X}}$ -modules which is faithful, exact and preserves small inductive limits. (In particular, $v(\mathbb{1}) = \mathcal{O}_{\mathcal{X}}$.)
- (F2) $M \in \mathcal{C}$ is dualizable whenever $v(M)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$ -module.

Remark 3.1. (i) The presence of a faithful functor $v : \mathcal{C} \rightarrow \mathbf{Qcoh}(\mathcal{X})$ as stated in (F1) already implies that all $\mathrm{Mor}_{\mathcal{C}}(M, N)$ are abelian groups, i.e. that \mathcal{C} is locally small. Hence, we could have omitted this condition in (C1). However, in this section and Section 4, we will not use conditions (F1) and (F2) and therefore need the condition “locally small” in (C1).

(ii) By an object $M \in \mathcal{C}$ being *dualizable*, we mean that M admits a (right) dual, i.e. an object $M^\vee \in \mathcal{C}$ together with two morphisms $\mathrm{ev}_M : M \otimes M^\vee \rightarrow \mathbb{1}$ (*evaluation*) and $\delta_M : \mathbb{1} \rightarrow M^\vee \otimes M$ (*coevaluation*) such that the diagrams

$$\begin{array}{ccc}
 M^\vee \cong \mathbb{1} \otimes M^\vee & \xrightarrow{\delta_M \otimes \mathrm{id}_{M^\vee}} & M^\vee \otimes M \otimes M^\vee \\
 & \searrow \mathrm{id}_{M^\vee} & \downarrow \mathrm{id}_{M^\vee} \otimes \mathrm{ev}_M \\
 & & M^\vee \otimes \mathbb{1} \cong M^\vee
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 M \cong M \otimes \mathbb{1} & \xrightarrow{\mathrm{id}_M \otimes \delta_M} & M \otimes M^\vee \otimes M \\
 & \searrow \mathrm{id}_M & \downarrow \mathrm{ev}_M \otimes \mathrm{id}_M \\
 & & \mathbb{1} \otimes M \cong M
 \end{array}$$

commute.

Example 3.2. All the settings mentioned in the introduction are examples for the category \mathcal{C} .

In the remainder of this section, \mathcal{C} will be a category satisfying properties (C1) and (C2).

Let $k := \mathrm{End}_{\mathcal{C}}(\mathbb{1})$ denote the ring of endomorphisms of the unit object $\mathbb{1}$. Then by simplicity of $\mathbb{1}$, k is a division ring, and even a field, as $\mathrm{End}_{\mathcal{C}}(\mathbb{1})$ is always commutative.

Let \mathbf{Vect}_k denote the category of k -vector spaces, and \mathbf{vect}_k the subcategory of finite dimensional k -vector spaces. There is a functor $\otimes_k : \mathcal{C} \times \mathbf{vect}_k \rightarrow \mathcal{C}$ such that $M \otimes_k k^n = M^n$ and in general $M \otimes_k V \cong M^{\dim(V)}$ (cf. [8], p. 21 for details).

As \mathcal{C} is cocomplete, the functor \otimes_k can be extended to $\otimes_k : \mathcal{C} \times \mathbf{Vect}_k \rightarrow \mathcal{C}$ via

$$M \otimes_k V := \varinjlim_{\substack{W \subseteq V \\ \text{fin. dim.}}} M \otimes_k W.$$

This functor fulfills a functorial isomorphism of k -vector spaces

$$\text{Mor}_{\mathcal{C}}(N, M \otimes_k V) \cong \text{Mor}_{\mathcal{C}}(N, M) \otimes_k V \text{ for all } M, N \in \mathcal{C}, V \in \mathbf{Vect}_k,$$

where the tensor product on the right hand side is the usual tensor product of k -vector spaces. Recall that $\text{Mor}_{\mathcal{C}}(N, M)$ is a k -vector space via the action of $k = \text{End}_{\mathcal{C}}(\mathbb{1})$.

The functor \otimes_k induces a tensor functor $\iota : \mathbf{Vect}_k \rightarrow \mathcal{C}$ given by $\iota(V) := \mathbb{1} \otimes_k V$, and one obviously has $M \otimes_k V \cong M \otimes \iota(V)$ (the second tensor product taken in \mathcal{C}). The functor ι is faithful and exact by construction. Since ι is an exact tensor functor and all finite dimensional vector spaces have a dual (in the categorical sense), all objects $\iota(V)$ for $V \in \mathbf{vect}_k$ are dualizable in \mathcal{C} .

There is also a functor $(-)^{\mathcal{C}} := \text{Mor}_{\mathcal{C}}(\mathbb{1}, -) : \mathcal{C} \rightarrow \mathbf{Vect}_k$ from the category \mathcal{C} to the category of all k -vector spaces.

Remark 3.3. As already mentioned in the introduction, in the differential case $M^{\mathcal{C}} = M^{\partial}$ is just the k -vector space of constants of the differential module M . In the difference case (with endomorphism σ), $M^{\mathcal{C}}$ equals the invariants M^{σ} of the difference module M .

The functor ι corresponds to the construction of “trivial” differential (resp. difference) modules by tensoring a k -vector space with the differential (resp. difference) base field F .

The following proposition gives some properties of the functors ι and $(-)^{\mathcal{C}}$ which are well known for differential resp. difference modules.

Proposition 3.4. *Let \mathcal{C} be a category satisfying (C1) and (C2), and let ι and $(-)^{\mathcal{C}}$ be as above. Then the following hold.*

- (i) *If $V \in \mathbf{Vect}_k$, then any subobject and any quotient of $\iota(V)$ is isomorphic to $\iota(W)$ for some $W \in \mathbf{Vect}_k$.*
- (ii) *If $V \in \mathbf{vect}_k$, then $\iota(V) \in \mathcal{C}$ has finite length and $\text{length}(\iota(V)) = \dim_k(V)$.*
- (iii) *If $M \in \mathcal{C}$ has finite length, then $M^{\mathcal{C}} \in \mathbf{vect}_k$ and $\dim_k(M^{\mathcal{C}}) \leq \text{length}(M)$.*

Proof. (i) First consider the case that $V \in \mathbf{Vect}_k$ is of finite dimension. We show the claim by induction on $\dim(V)$.

The case $\dim(V) = 0$ is trivial. Let $V \in \mathbf{vect}_k$ and $N \in \mathcal{C}$ be a subobject of $\iota(V)$, and let $V' \subseteq V$ be a 1-dimensional subspace. Then one has a split exact sequence of k -vector spaces $0 \rightarrow V' \rightarrow V \rightarrow V/V' \rightarrow 0$ and therefore a split exact sequence

$$0 \rightarrow \iota(V') \rightarrow \iota(V) \rightarrow \iota(V/V') \rightarrow 0$$

in \mathcal{C} . Since N is a subobject of $\iota(V)$, the pullback $N \cap \iota(V')$ is a subobject of $\iota(V') \cong \mathbb{1}$. As $\mathbb{1}$ is simple, $N \cap \iota(V') = 0$ or $N \cap \iota(V') = \iota(V')$.

In the first case, $N \hookrightarrow \iota(V/V')$, and the claim follows by induction on $\dim(V)$.

In the second case, by induction $N/\iota(V')$ is isomorphic to $\iota(W)$ for some subspace $W \subseteq \iota(V/V')$. If W' denotes the preimage of W under the epimorphism $V \rightarrow V/V'$, one has a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \iota(V') & \longrightarrow & N & \longrightarrow & \iota(W) \longrightarrow 0, \\ & & \downarrow \cong & & \downarrow & & \downarrow \cong \\ 0 & \longrightarrow & \iota(V') & \longrightarrow & \iota(W') & \longrightarrow & \iota(W) \longrightarrow 0 \end{array}$$

and therefore $N \cong \iota(W')$.

If $V \in \mathbf{Vect}_k$ has infinite dimension, we recall that $\iota(V) = \varinjlim_{\substack{W \subseteq V \\ \text{fin.dim.}}} \iota(W)$

and hence, for any subobject $N \subseteq \iota(V)$, one has

$$N = \varinjlim_{\substack{W \subseteq V \\ \text{fin.dim.}}} N \cap \iota(W).$$

From the special case of finite dimension, we obtain $N \cap \iota(W) = \iota(W')$ for some W' related to W , and therefore

$$N = \varinjlim_{\substack{W \subseteq V \\ \text{fin.dim.}}} \iota(W') = \iota \left(\varinjlim_{\substack{W \subseteq V \\ \text{fin.dim.}}} W' \right).$$

Now let $V \in \mathbf{Vect}_k$ be arbitrary and, let N be a quotient of $\iota(V)$. Then by the previous, $\text{Ker}(\iota(V) \rightarrow N)$ is of the form $\iota(V')$ for some $V' \subseteq V$, and hence $N \cong \iota(V)/\iota(V') \cong \iota(V/V')$, as ι is exact.

- (ii) By part (i), every sequence of subobjects $0 = N_0 \subsetneq N_1 \subsetneq \dots \subsetneq \iota(V)$ is induced via ι by a sequence of subvector spaces $0 = W_0 \subsetneq W_1 \subsetneq \dots \subsetneq V$. Hence, $\text{length}(\iota(V)) = \dim_k(V)$.
- (iii) We use induction on the length of M . If M has length 1, then M is a simple object. Since $\mathbb{1}$ also is simple, every morphism in $M^{\mathcal{C}} = \text{Mor}_{\mathcal{C}}(\mathbb{1}, M)$ is either 0 or an isomorphism. In particular, $k = \text{End}_{\mathcal{C}}(\mathbb{1})$ acts transitively on $\text{Mor}_{\mathcal{C}}(\mathbb{1}, M)$, which shows that $\dim_k(\text{Mor}_{\mathcal{C}}(\mathbb{1}, M))$ is 0 or 1. For the general case, take a subobject $0 \neq N \neq M$ of M . Applying the functor $()^{\mathcal{C}} = \text{Mor}_{\mathcal{C}}(\mathbb{1}, -)$ to the exact sequence $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ leads to an exact sequence

$$0 \rightarrow N^{\mathcal{C}} \rightarrow M^{\mathcal{C}} \rightarrow (M/N)^{\mathcal{C}},$$

as the functor $\text{Mor}_{\mathcal{C}}(X, -)$ is always left-exact.

Hence, $\dim_k(M^{\mathcal{C}}) \leq \dim_k(N^{\mathcal{C}}) + \dim_k((M/N)^{\mathcal{C}})$. Since N and M/N have smaller length than M , we obtain the claim by induction using $\text{length}(M) = \text{length}(N) + \text{length}(M/N)$.

□

Proposition 3.5. *Let \mathcal{C} be a category satisfying (C1) and (C2) and let ι and $()^{\mathcal{C}}$ be as above. Then the following hold.*

- (i) *The functor ι is left adjoint to the functor $()^{\mathcal{C}}$, i.e. for all $V \in \mathbf{Vect}_k$, $M \in \mathcal{C}$, there are isomorphisms of k -vector spaces $\text{Mor}_{\mathcal{C}}(\iota(V), M) \cong \text{Hom}_k(V, M^{\mathcal{C}})$ functorial in V and M .*

- (ii) For every $V \in \mathbf{Vect}_k$, the homomorphism $\eta_V : V \rightarrow (\iota(V))^{\mathcal{C}}$ which is adjoint to $\text{id}_{\iota(V)}$ is an isomorphism.
- (iii) For every $M \in \mathcal{C}$, the morphism $\varepsilon_M : \mathbf{1} \otimes_k \text{Mor}_{\mathcal{C}}(\mathbf{1}, M) = \iota(M^{\mathcal{C}}) \rightarrow M$ which is adjoint to $\text{id}_{M^{\mathcal{C}}}$ is a monomorphism.

Remark 3.6. (i) Whereas in the differential resp. difference settings, part (i) and (ii) are easily seen, part (iii) amounts to saying that any set $v_1, \dots, v_n \in M^{\mathcal{C}}$ of constant (resp. invariant) elements of M which are k -linearly independent, are also independent over the differential (resp. difference) field F . This is proven in each setting separately. However, Amano and Masuoka provide an abstract proof (which is given in [1, Prop. 3.1.1]) which relies on the Freyd embedding theorem.

(ii) The collection of homomorphisms $(\eta_V)_{V \in \mathbf{Vect}_k}$ is just the natural transformation $\eta : \text{id}_{\mathbf{Vect}_k} \rightarrow (-)^{\mathcal{C}} \circ \iota$ (unit of the adjunction) whereas the morphisms ε_M form the natural transformation $\varepsilon : \iota \circ (-)^{\mathcal{C}} \rightarrow \text{id}_{\mathcal{C}}$ (counit of the adjunction). By the general theory on adjoint functors, for all $V, W \in \mathbf{Vect}_k$, the maps $\text{Hom}_k(V, W) \rightarrow \text{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$ induced by applying ι are just the compositions

$$\text{Hom}_k(V, W) \xrightarrow{\eta_W \circ (-)} \text{Hom}_k(V, \iota(W)^{\mathcal{C}}) \xleftarrow[\simeq]{\text{adjunction}} \text{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$$

(cf. [14], p. 81, eq. (3) and definition of η). This implies that η_W is a monomorphism for all $W \in \mathbf{Vect}_k$ if and only if $\text{Hom}_k(V, W) \rightarrow \text{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$ is injective for all $V, W \in \mathbf{Vect}_k$, i.e. if ι is a faithful functor. Furthermore, η_W is a split epimorphism for all $W \in \mathbf{Vect}_k$ if and only if $\text{Hom}_k(V, W) \rightarrow \text{Mor}_{\mathcal{C}}(\iota(V), \iota(W))$ is surjective for all $V, W \in \mathbf{Vect}_k$, if and only if ι is a full functor. In particular, η_W being an isomorphism for all $W \in \mathbf{Vect}_k$ is equivalent to ι being a fully faithful functor.

Proof of Prop. 3.5. (i) For $V \in \mathbf{vect}_k$ and $M \in \mathcal{C}$ we have natural isomorphisms

$$\begin{aligned} \text{Mor}_{\mathcal{C}}(\iota(V), M) &\cong \text{Mor}_{\mathcal{C}}(\mathbf{1}, M \otimes \iota(V)^{\vee}) \cong \text{Mor}_{\mathcal{C}}(\mathbf{1}, M \otimes_k V^{\vee}) \\ &\cong \text{Mor}_{\mathcal{C}}(\mathbf{1}, M) \otimes_k V^{\vee} \cong \text{Hom}_k(V, \text{Mor}_{\mathcal{C}}(\mathbf{1}, M)) \\ &= \text{Hom}_k(V, M^{\mathcal{C}}) \end{aligned}$$

If V is of infinite dimension the statement is obtained using that $\text{Mor}_{\mathcal{C}}$ and Hom_k commute with inductive limits, i.e.

$$\begin{aligned} \text{Mor}_{\mathcal{C}}(\iota(V), M) &= \text{Mor}_{\mathcal{C}}(\varinjlim_{\substack{W \subset V \\ \text{fin. dim}}} \iota(W), M) = \varprojlim_{\substack{W \subset V \\ \text{fin. dim}}} \text{Mor}_{\mathcal{C}}(\iota(W), M) \\ &\cong \varprojlim_{\substack{W \subset V \\ \text{fin. dim}}} \text{Hom}_k(W, M^{\mathcal{C}}) = \text{Hom}_k(V, M^{\mathcal{C}}). \end{aligned}$$

- (ii) We have, $(\iota(V))^{\mathcal{C}} = \text{Mor}_{\mathcal{C}}(\mathbf{1}, \mathbf{1} \otimes_k V) \cong \text{Mor}_{\mathcal{C}}(\mathbf{1}, \mathbf{1}) \otimes_k V \cong k \otimes_k V = V$, and the morphism $\text{id}_{\iota(V)}$ corresponds to $\text{id}_V : V \xrightarrow{\eta_V} (\iota(V))^{\mathcal{C}} \cong V$ via all these natural identifications.

- (iii) Let $M \in \mathcal{C}$ and $N := \text{Ker}(\varepsilon_M) \subseteq \iota(M^{\mathcal{C}})$. By Prop. 3.4(i), there is a subspace W of $M^{\mathcal{C}}$ such that $N = \iota(W)$. Hence, we have an exact sequence of morphisms

$$0 \rightarrow \iota(W) \rightarrow \iota(M^{\mathcal{C}}) \xrightarrow{\varepsilon_M} M.$$

Since $()^{\mathcal{C}}$ is left exact, this leads to the exact sequence

$$0 \rightarrow (\iota(W))^{\mathcal{C}} \rightarrow (\iota(M^{\mathcal{C}}))^{\mathcal{C}} \xrightarrow{(\varepsilon_M)^{\mathcal{C}}} M^{\mathcal{C}}$$

But $\eta_V : V \rightarrow (\iota(V))^{\mathcal{C}}$ is an isomorphism for all V by part (ii). So we obtain an exact sequence

$$0 \rightarrow W \rightarrow M^{\mathcal{C}} \xrightarrow{(\varepsilon_M)^{\mathcal{C}} \circ \eta_{M^{\mathcal{C}}}} M^{\mathcal{C}},$$

and the composite $(\varepsilon_M)^{\mathcal{C}} \circ \eta_{M^{\mathcal{C}}}$ is the identity on $M^{\mathcal{C}}$ by general theory on adjoint functors (cf. [14, Ch. IV, Thm. 1]). Hence, $W = 0$. \square

4. \mathcal{C} -ALGEBRAS AND BASE CHANGE

We recall some notation which are already present in [13, Ch. 17 & 18], and refer to loc. cit. for more details. The reader should be aware that a “tensor category” in [13] is the same as an “abelian symmetric monoidal category” here. A **commutative algebra in \mathcal{C}** (or a **\mathcal{C} -algebra** for short) is an object $R \in \mathcal{C}$ together with two morphisms $u_R : \mathbb{1} \rightarrow R$ and $\mu_R : R \otimes R \rightarrow R$ satisfying several commuting diagrams corresponding to associativity, commutativity and the unit. For instance,

$$\mu_R \circ (u_R \otimes \text{id}_R) = \text{id}_R = \mu_R \circ (\text{id}_R \otimes u_R)$$

says that u_R is a unit for the multiplication μ_R (cf. [13, Ch. 17]; although the term “ \mathcal{C} -algebra” in [13] does not include commutativity).

For a \mathcal{C} -algebra R we define \mathcal{C}_R to be the category of R -modules in \mathcal{C} , i.e. the category of pairs (M, μ_M) where $M \in \mathcal{C}$ and $\mu_M : R \otimes M \rightarrow M$ is a morphism in \mathcal{C} satisfying the usual commuting diagrams for turning M into an R -module (cf. [13, Ch. 18]).³ The morphisms in \mathcal{C}_R are morphisms in \mathcal{C} which commute with the R -action. The category \mathcal{C}_R is also an abelian symmetric monoidal category with tensor product \otimes_R defined as

$$M \otimes_R N := \text{Coker}((\mu_M \circ \tau) \otimes \text{id}_N - \text{id}_M \otimes \mu_N : M \otimes R \otimes N \rightarrow M \otimes N),$$

where $\tau : M \otimes R \rightarrow R \otimes M$ is the twist morphism (see [13, Prop. 18.3]).

A **\mathcal{C} -ideal** I of a \mathcal{C} -algebra R is a subobject of R in the category \mathcal{C}_R , and R is called a **simple \mathcal{C} -algebra**, if 0 and R are the only \mathcal{C} -ideals of R , i.e. if R is a simple object in \mathcal{C}_R .

Definition 4.1. For a \mathcal{C} -algebra R , the additive right-exact functor $()_R : (\mathcal{C}, \otimes) \rightarrow (\mathcal{C}_R, \otimes_R), M \mapsto M_R := (R \otimes M, \mu_R \otimes \text{id}_M)$ is called the *base change functor*. It is even a tensor functor, and it is a left adjoint to the forgetful functor $\mathcal{C}_R \rightarrow \mathcal{C}$ (see [13, Thm. 18.2]).

³Most times, we will omit the μ_M in our notation, and just write $M \in \mathcal{C}_R$.

We can also base change the functors ι and $()^{\mathcal{C}}$. In more details, having in mind that $\text{End}_{\mathcal{C}_R}(R) = \text{Mor}_{\mathcal{C}}(\mathbb{1}, R) = R^{\mathcal{C}}$:

$$\iota_R : \text{Mod}_{R^{\mathcal{C}}} \rightarrow \mathcal{C}_R, V \mapsto R \otimes_{\iota(R^{\mathcal{C}})} \iota(V)$$

and

$$()^{\mathcal{C}_R} : \mathcal{C}_R \rightarrow \text{Mod}_{R^{\mathcal{C}}}, M \mapsto \text{Mor}_{\mathcal{C}_R}(R, M) = \text{Mor}_{\mathcal{C}}(\mathbb{1}, M) = M^{\mathcal{C}}.$$

A special case is given, if $R = \iota(A)$ for some commutative k -algebra A . In this case, ι_R is “the same” as ι . This case corresponds to an extension by constants in the theory of differential or difference modules.

Proposition 4.2. *The functor ι_R is left adjoint to the functor $()^{\mathcal{C}_R}$.*

Proof. Let $V \in \text{Mod}_{R^{\mathcal{C}}}$ and $M \in \mathcal{C}_R$, then

$$\text{Mor}_{\mathcal{C}_R}(\iota_R(V), M) = \text{Mor}_{\mathcal{C}_R}(R \otimes_{\iota(R^{\mathcal{C}})} \iota(V), M) = \text{Mor}_{\mathcal{C}_{\iota(R^{\mathcal{C}})}}(\iota(V), M)$$

is the subset of $\text{Mor}_{\mathcal{C}}(\iota(V), M)$ given by all $f \in \text{Mor}_{\mathcal{C}}(\iota(V), M)$ such that the diagram

$$\begin{array}{ccc} \iota(R^{\mathcal{C}}) \otimes \iota(V) & \xrightarrow{\text{id} \otimes f} & \iota(R^{\mathcal{C}}) \otimes M \\ \downarrow \iota(\mu_V) & & \downarrow \mu_M \\ \iota(V) & \xrightarrow{f} & M \end{array}$$

commutes. On the other hand, $\text{Hom}_{R^{\mathcal{C}}}(V, M^{\mathcal{C}_R}) = \text{Hom}_{R^{\mathcal{C}}}(V, M^{\mathcal{C}})$ is the subset of $\text{Hom}_k(V, M^{\mathcal{C}})$ given by all $g \in \text{Hom}_k(V, M^{\mathcal{C}})$ such that the diagram

$$\begin{array}{ccc} R^{\mathcal{C}} \otimes_k V & \xrightarrow{\text{id} \otimes g} & R^{\mathcal{C}} \otimes_k M^{\mathcal{C}} \\ \downarrow \mu_V & & \downarrow (\mu_M)^{\mathcal{C}} \\ V & \xrightarrow{g} & M^{\mathcal{C}} \end{array}$$

commutes. Assume that f and g are adjoint morphisms (i.e. correspond to each other via the bijection $\text{Mor}_{\mathcal{C}}(\iota(V), M) \cong \text{Hom}_k(V, M^{\mathcal{C}})$ of Prop.3.5(i)), then the commutativity of the first diagram is equivalent to the commutativity of the second, since the bijection of the hom-sets is natural. \square

Lemma 4.3. *Let A be a commutative k -algebra. Then $\iota_{\iota(A)}$ and $()^{\mathcal{C}_{\iota(A)}}$ define a bijection between the ideals of A and the \mathcal{C} -ideals of $\iota(A)$.*

Proof. By definition $\iota_{\iota(A)}(I) = \iota(I)$ for any $I \in \text{Mod}_A$. Furthermore, by Prop. 3.4(i), ι induces a bijection between the k -subvector spaces of A and the subobjects of $\iota(A)$ in \mathcal{C} . The condition on I being an ideal of A (resp. of $\iota(I)$ being an ideal of $\iota(A)$) is equivalent to the condition that the composite $A \otimes_k I \xrightarrow{\mu_A} A \rightarrow A/I$ (resp. the composite $\iota(A) \otimes \iota(I) \xrightarrow{\mu_{\iota(A)}} \iota(A) \rightarrow \iota(A)/\iota(I)$) is the zero map. Hence, the condition for $\iota(I)$ is obtained from the one for I by applying ι , and using that ι is an exact tensor functor. Since ι is also faithful, these two conditions are indeed equivalent. \square

In the special case that A is a field, one obtains the following corollary.

Corollary 4.4. *Let ℓ be a field extension of k , then $\iota(\ell)$ is a simple \mathcal{C} -algebra.*

Remark 4.5. As ι_R and $()^{\mathcal{C}_R}$ are adjoint functors, there are again the unit and the counit of the adjunction. By abuse of notation, we will again denote the unit by η and the counit by ε . There might be an ambiguity which morphism is meant by ε_M if (M, μ_M) is an object in \mathcal{C}_R . However, when M is explicitly given as an object of \mathcal{C}_R , then $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \rightarrow M$ is meant. This is the case, for example, if $M = N_R$ is the base change of an object $N \in \mathcal{C}$. In cases where the right meaning of ε_M would not be clear, we always give the source and the target of ε_M .

Proposition 4.6. *Assume that, ι_R is exact and faithful⁴, and that any subobject of R^n is of the form $\iota_R(W)$, then the following holds.*

- (i) *For every $V \in \mathbf{Mod}_{R^{\mathcal{C}}}$, every subobject of $\iota_R(V)$ is isomorphic to $\iota_R(W)$ for some $W \subseteq V$.*
- (ii) *For every $V \in \mathbf{Mod}_{R^{\mathcal{C}}}$, the morphism $\eta_V : V \rightarrow (\iota_R(V))^{\mathcal{C}_R}$ is an isomorphism.*
- (iii) *For every $M \in \mathcal{C}_R$, the morphism $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \rightarrow M$ is a monomorphism.*

The most important cases where the proposition applies is on the one hand the case $R = \iota(A)$ for some commutative k -algebra A (in which case $\iota_R = \iota$), and on the other hand R being a simple \mathcal{C} -algebra.

Proof. (ii) We show that $\eta_V : V \rightarrow (\iota_R(V))^{\mathcal{C}_R}$ is an isomorphism for all $V \in \mathbf{Mod}_{R^{\mathcal{C}}}$. As ι is faithful by assumption, all η_V are monomorphisms (cf. Rem. 3.6). For showing that η_V is an epimorphism, it is enough to show that the natural map

$$R^{\mathcal{C}} \otimes_k V = (R \otimes \iota(V))^{\mathcal{C}_R} \rightarrow (\iota_R(V))^{\mathcal{C}_R}$$

is an epimorphism, where on the left hand side, V is considered just as a k -vector space. Saying that this map is epimorphic is equivalent to saying that any morphism $g : R \rightarrow \iota_R(V)$ in \mathcal{C}_R can be lifted to a morphism $f : R \rightarrow R \otimes \iota(V)$ in \mathcal{C}_R . So let $g : R \rightarrow \iota_R(V)$ be a morphism in \mathcal{C}_R , and let P be the pullback of the diagram

$$\begin{array}{ccc} P & \xrightarrow{\text{pr}_1} & R \\ \downarrow \text{pr}_2 & & \downarrow g \\ R \otimes \iota(V)^p & \xrightarrow{\quad} & \iota_R(V) \end{array} .$$

Then P is a subobject of $R \oplus (R \otimes \iota(V)) \cong R^{1+\dim_k(V)}$, and hence by assumption, $P = \iota_R(W)$ for some $W \in \mathbf{Mod}_{R^{\mathcal{C}}}$. By adjointness, pr_1 corresponds to some $R^{\mathcal{C}}$ -homomorphism $q : W \rightarrow R^{\mathcal{C}_R} = R^{\mathcal{C}}$, i.e. $\text{pr}_1 = \varepsilon_R \circ \iota_R(q)$. Since $\varepsilon_R : R = \iota_R(R^{\mathcal{C}_R}) \rightarrow R$ is the identity, and pr_1 is an epimorphism, faithfulness of ι_R implies that also q is an epimorphism. Therefore, there is a $R^{\mathcal{C}}$ -homomorphism $s : R^{\mathcal{C}} \rightarrow W$ such that $q \circ s = \text{id}_{R^{\mathcal{C}}}$. Let f be the morphism $f := \text{pr}_2 \circ \iota_R(s) : R \rightarrow R \otimes \iota(V)$, then

$$p \circ f = p \circ \text{pr}_2 \circ \iota_R(s) = g \circ \text{pr}_1 \circ \iota_R(s) = g \circ \iota_R(q \circ s) = g.$$

⁴For differential rings this means that the ring R is faithfully flat over $\iota(R^{\mathcal{C}})$.

Hence, f is a lift of g .

- (i) We show that any subobject of $\iota_R(V)$ is of the form $\iota_R(W)$ for some submodule W of V . The case of a quotient of $\iota_R(V)$ then follows in the same manner as in Prop. 3.4. Let $N \subseteq \iota_R(V)$ be a subobject in \mathcal{C}_R . Then the pullback of N along $p : R \otimes \iota(V) \rightarrow \iota_R(V)$ is a subobject of $R \otimes \iota(V)$, hence by assumption of the form $\iota_R(\tilde{W})$ for some $\tilde{W} \subseteq (R^{\mathcal{C}})^{\dim_k(V)}$. Furthermore, as η_V is an isomorphism, the restriction $p|_{\iota_R(\tilde{W})} : \iota_R(\tilde{W}) \rightarrow \iota_R(V)$ is induced by some homomorphism $f : \tilde{W} \rightarrow V$ (cf. Remark 3.6). By exactness of ι_R , we finally obtain $N = \text{Im}(\iota_R(f)) = \iota_R(\text{Im}(f)) = \iota_R(W)$ for $W := \text{Im}(f)$.
- (iii) The proof that $\varepsilon_M : \iota_R(M^{\mathcal{C}_R}) \rightarrow M$ is a monomorphism is the same as in Prop. 3.5.

□

Lemma 4.7. *Let R be a simple \mathcal{C} -algebra. Then for $N \in \mathcal{C}_R$, the morphism ε_N is an isomorphism if and only if N is isomorphic to $\iota_R(V)$ for some $V \in \mathbf{Mod}_{R^{\mathcal{C}}}$.*

Proof. If ε_N is an isomorphism, then $N \cong \iota_R(V)$ for $V := N^{\mathcal{C}_R}$. On the other hand, let $N \cong \iota_R(V)$ for some $V \in \mathbf{Mod}_{R^{\mathcal{C}}}$. Since $\iota_R(\eta_V) \circ \varepsilon_{\iota_R(V)} = \text{id}_{\iota_R(V)}$ (cf. [14, Ch. IV, Thm. 1]) and η_V is an isomorphism, $\varepsilon_{\iota_R(V)}$ is an isomorphism. Hence, ε_N is an isomorphism. □

Proposition 4.8. *Let R be a simple \mathcal{C} -algebra. Then the full subcategory of \mathcal{C}_R consisting of all $N \in \mathcal{C}_R$ such that ε_N is an isomorphism is a monoidal subcategory of \mathcal{C}_R and is closed under taking direct sums, subquotients, small inductive limits, and duals of dualizable objects in \mathcal{C}_R .*

Proof. Using the previous lemma, this follows directly from Prop. 4.6(i), and the fact that ι_R is an additive exact tensor functor. □

5. SOLUTION RINGS AND PICARD-VESSIOT RINGS

From now on we assume that \mathcal{C} satisfies all conditions (C1), (C2), (F1) and (F2).

Lemma 5.1. *Let $M \in \mathcal{C}$ be dualizable. Then $v(M)$ is a finitely generated locally free $\mathcal{O}_{\mathcal{X}}$ -module of constant rank.*

Proof. If $M \in \mathcal{C}$ is dualizable, then $v(M)$ is dualizable in $\mathbf{Qcoh}(\mathcal{X})$, since v is a tensor functor, and tensor functors map dualizable objects to dualizable objects (and their duals to the duals of the images). By [7, Prop. 2.6], dualizable objects in $\mathbf{Qcoh}(\mathcal{X})$ are exactly the finitely generated locally free $\mathcal{O}_{\mathcal{X}}$ -modules. Hence, $v(M)$ is finitely generated and locally free whenever M is dualizable.

To see that the rank is constant, let $d \in \mathbb{N}$ be the maximal local rank of $v(M)$, and consider the d -th exterior power $\Lambda := \Lambda^d(M) \in \mathcal{C}$ which is non-zero by the choice of d . Hence, the evaluation morphism $\text{ev}_{\Lambda} : \Lambda \otimes \Lambda^{\vee} \rightarrow \mathbb{1}$ is non-zero. Since $\mathbb{1}$ is simple, and the image of ev_{Λ} is a subobject of $\mathbb{1}$, the morphism ev_{Λ} is indeed an epimorphism. Hence the evaluation

$$\text{ev}_{v(\Lambda)} = v(\text{ev}_{\Lambda}) : v(\Lambda) \otimes_{\mathcal{O}_{\mathcal{X}}} v(\Lambda)^{\vee} \rightarrow \mathcal{O}_{\mathcal{X}}$$

is surjective which implies that $v(\Lambda) \otimes_{\mathcal{O}_{\mathcal{X}}} \mathcal{O}_{\mathcal{X},x} \neq 0$ for any point x of \mathcal{X} . But this means that any local rank of $v(M)$ is at least d , i.e. $v(M)$ has constant rank d . \square

Remark 5.2. With respect to the previous lemma, condition (F2) implies that if $v(M)$ is finitely generated for some $M \in \mathcal{C}$, then $v(M)$ is even locally free and of constant rank. This also implies the following:

If M is dualizable, then $v(M)$ is finitely generated and locally free. Further, for every epimorphic image N of M , the $\mathcal{O}_{\mathcal{X}}$ -module $v(N)$ is also finitely generated and hence, locally free. But then for any subobject $N' \subseteq M$ the sequence $0 \rightarrow v(N') \rightarrow v(M) \rightarrow v(M/N') \rightarrow 0$ is split exact, since $v(M/N')$ as an epimorphic image is locally free. Therefore $v(N')$ is also a quotient of $v(M)$, in particular $v(N')$ is finitely generated and locally free.

So given a dualizable $M \in \mathcal{C}$, all subquotients of finite direct sums of objects $M^{\otimes n} \otimes (M^{\vee})^{\otimes m}$ ($n, m \in \mathbb{N}$) are dualizable. Hence, the strictly full tensor subcategory of \mathcal{C} generated by M and M^{\vee} – which is exactly the full subcategory of \mathcal{C} consisting of all objects isomorphic to subquotients of finite direct sums of objects $M^{\otimes n} \otimes (M^{\vee})^{\otimes m}$ ($n, m \in \mathbb{N}$) – is a rigid abelian tensor category and will be denoted by $\langle\langle M \rangle\rangle$. Furthermore by definition, v is a fibre functor and therefore $\langle\langle M \rangle\rangle$ is even a Tannakian category (cf. [7, Section 2.8]).

By [7, Cor. 6.20], there exists a finite extension \tilde{k} of k and a fibre functor $\omega : \langle\langle M \rangle\rangle \rightarrow \mathbf{vect}_{\tilde{k}}$. In view of Thm. 6.5 in Section 6, this implies that there is a Picard-Vessiot ring for M over \tilde{k} .

We will see later (cf. Cor. 5.13) that for every simple minimal solution ring R , the field $R^{\mathcal{C}} = \text{End}_{\mathcal{C}_R}(R)$ is a finite field extension of k .

Definition 5.3. Let $M \in \mathcal{C}$.

A *solution ring* for M is a \mathcal{C} -algebra R such that the morphism

$$\varepsilon_{M_R} : \iota_R((M_R)^{\mathcal{C}_R}) \rightarrow M_R = R \otimes M$$

is an isomorphism.

A *Picard-Vessiot ring* for M is a minimal solution ring R which is a simple \mathcal{C} -algebra, and satisfies $R^{\mathcal{C}} := \text{End}_{\mathcal{C}_R}(R) = k$. Here, *minimal* means that for any solution ring $\tilde{R} \in \mathcal{C}$ that admits a monomorphism of \mathcal{C} -algebras to R , this monomorphism is indeed an isomorphism.

Remark 5.4. Comparing with the differential setting, $(M_R)^{\mathcal{C}_R}$ is just the so called solution space $(R \otimes_F M)^{\partial}$ of M over R , and ε_{M_R} is the canonical homomorphism $R \otimes_{R^{\partial}} (R \otimes_F M)^{\partial} \rightarrow R \otimes_F M$.

When R is a simple \mathcal{C} -algebra (i.e. in the differential setting a simple differential ring), then by Prop.4.6(iii), ε_{M_R} is always a monomorphism. Hence, for a simple \mathcal{C} -algebra R , the condition for being a solution ring means that the solution space is as large as possible, or in other words that $R \otimes M$ has a basis of constant elements, i.e. is a trivial differential module over R .

Proposition 5.5. Let R be a solution ring for some dualizable $M \in \mathcal{C}$, and let $f : R \rightarrow R'$ be an epimorphism of \mathcal{C} -algebras. Assume either that R' is a simple \mathcal{C} -algebra or that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$ -module. Then R' is a solution ring for M as well.

Remark 5.6. If $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$ -module, then it is automatically free of finite rank, and the rank is the same as the global rank of $v(M)$ as $\mathcal{O}_{\mathcal{X}}$ -module which exists by Lem. 5.1.

Proof of Prop. 5.5. As $f : R \rightarrow R'$ is an epimorphism and M is dualizable, $f \otimes \text{id}_M : R \otimes M \rightarrow R' \otimes M$ is an epimorphism, too. As the diagram

$$\begin{array}{ccc} \iota_R((R \otimes M)^{\mathcal{C}}) & \xrightarrow{\varepsilon_{M_R}} & M_R = R \otimes M \\ \downarrow & & \downarrow f \otimes \text{id}_M \\ \iota_{R'}((R' \otimes M)^{\mathcal{C}}) & \xrightarrow{\varepsilon_{M_{R'}}} & M_{R'} = R' \otimes M \end{array}$$

commutes and ε_{M_R} is an isomorphism by assumption on R , the morphism $\varepsilon_{M_{R'}}$ is an epimorphism.

If R' is simple, then by Prop. 4.6(iii) the morphism $\varepsilon_{M_{R'}}$ is a monomorphism, hence an isomorphism. Therefore, R' is a solution ring.

Assume now, that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$ -module of rank n . Then $\iota_R(R \otimes M)^{\mathcal{C}} \cong \iota_R((R^{\mathcal{C}})^n) = R^n$. Composing with ε_{M_R} leads to an isomorphism $R^n \xrightarrow{\cong} R \otimes M$. We therefore obtain an isomorphism $\alpha : (R')^n \rightarrow R' \otimes M$ by tensoring with R' . Applying the natural transformation ε to this isomorphism, we get a commutative square

$$\begin{array}{ccc} R'^n = \iota_{R'}((R')^n)^{\mathcal{C}} & \xrightarrow[\cong]{\iota_{R'}(\alpha^{\mathcal{C}})} & \iota_{R'}((R' \otimes M)^{\mathcal{C}}) \\ \cong \downarrow \varepsilon_{R'^n} & & \downarrow \varepsilon_{M_{R'}} \\ R'^n & \xrightarrow[\cong]{\alpha} & R' \otimes M, \end{array}$$

which shows that $\varepsilon_{M_{R'}}$ is an isomorphism, too. \square

Theorem 5.7. *Let $M \in \mathcal{C}$ be dualizable. Then there exists a non-zero solution ring for M .*

Proof. We show the theorem by explicitly constructing a solution ring. This construction is motivated by the Tannakian point of view in [8] and by Section 3.4 in [3].

Let $n := \text{rank}(v(M))$ be the global rank of the $\mathcal{O}_{\mathcal{X}}$ -module $v(M)$ which exists by Lemma 5.1. We then define U to be the residue ring of $\text{Sym}\left((M \otimes (\mathbb{1}^n)^{\vee}) \oplus (\mathbb{1}^n \otimes M^{\vee})\right)$ subject to the ideal generated by the image of the morphism

$$\begin{aligned} (-\text{ev}, \text{id}_M \otimes \delta_{\mathbb{1}^n} \otimes \text{id}_{M^{\vee}}) : M \otimes M^{\vee} &\rightarrow \mathbb{1} \oplus (M \otimes (\mathbb{1}^n)^{\vee} \otimes \mathbb{1}^n \otimes M^{\vee}) \\ &\subset \text{Sym}\left((M \otimes (\mathbb{1}^n)^{\vee}) \oplus (\mathbb{1}^n \otimes M^{\vee})\right). \end{aligned}$$

First we show that $U \neq 0$ by showing $v(U) \neq 0$. By exactness of v , the ring $v(U)$ is given as the residue ring of $\text{Sym}((v(M) \otimes_{\mathcal{O}_{\mathcal{X}}} (\mathcal{O}_{\mathcal{X}}^n)^{\vee}) \oplus (\mathcal{O}_{\mathcal{X}}^n \otimes_{\mathcal{O}_{\mathcal{X}}} v(M)^{\vee}))$ subject to the ideal generated by the image of $(-\text{ev}_{v(M)}, \text{id} \otimes \delta_{\mathcal{O}_{\mathcal{X}}^n} \otimes \text{id})$.

Let $\mathcal{U} = \text{Spec}(S) \subseteq \mathcal{X}$ be an affine open subset such that $\tilde{M} := v(M)(\mathcal{U})$ is free over S . Let $\{b_1, \dots, b_n\}$ be a basis of \tilde{M} and $b_1^{\vee}, \dots, b_n^{\vee} \in \tilde{M}^{\vee}$ the corresponding

dual basis. Then $v(U)(\mathcal{U})$ is generated by $x_{ij} := b_i \otimes e_j^\vee \in \tilde{M} \otimes (S^n)^\vee$ and $y_{ji} := e_j \otimes b_i^\vee \in S^n \otimes (\tilde{M})^\vee$ for $i, j = 1, \dots, n$, where $\{e_1, \dots, e_n\}$ denotes the standard basis of S^n and $\{e_1^\vee, \dots, e_n^\vee\}$ the dual basis. The relations are generated by

$$b_k^\vee(b_i) = \text{ev}_{\tilde{M}}(b_i \otimes b_k^\vee) = (\text{id}_{\tilde{M}} \otimes \delta_{S^n} \otimes \text{id}_{\tilde{M}^\vee})(b_i \otimes b_k^\vee) = \sum_{j=1}^n (b_i \otimes e_j^\vee) \otimes (e_j \otimes b_k^\vee),$$

i.e. $\delta_{ik} = \sum_{j=1}^n x_{ij} y_{jk}$ for all $i, k = 1, \dots, n$. This just means that the matrix $Y = (y_{jk})$ is the inverse of the matrix $X = (x_{ij})$. Hence $v(U)(\mathcal{U}) = S[X, X^{-1}]$ is the localisation of a polynomial ring over S in n^2 variables.

For showing that U is indeed a solution ring, we consider the following diagram

$$\begin{array}{ccccc}
M & \xrightarrow{\text{id}_M \otimes \delta_{\mathbb{1}^n}} & (M \otimes (\mathbb{1}^n)^\vee) \otimes \mathbb{1}^n & \xrightarrow{\text{incl.} \otimes \text{id}_{\mathbb{1}^n}} & U \otimes \mathbb{1}^n \\
\downarrow \text{id}_M \otimes \delta_M & & \downarrow \text{id} \otimes \delta_M & & \downarrow \text{id} \otimes \delta_M \\
M \otimes M^\vee \otimes M & \xrightarrow{\text{id}_M \otimes \delta_{\mathbb{1}^n} \otimes \text{id}} & (M \otimes (\mathbb{1}^n)^\vee) \otimes (\mathbb{1}^n \otimes M^\vee) \otimes M & \xrightarrow{\text{incl.} \otimes \text{id}} & U \otimes (\mathbb{1}^n \otimes M^\vee) \otimes M \\
\downarrow \text{ev}_M \otimes \text{id}_M & & \downarrow \mu_U \otimes \text{id}_M & & \downarrow \mu_U \otimes \text{id}_M \\
\mathbb{1} \otimes M & \xrightarrow{u_U \otimes \text{id}_M} & U \otimes M & \xrightarrow{\text{id}} & U \otimes M.
\end{array}$$

It is easy to see that the upper left, upper right and lower right squares all commute. The lower left square also commutes by definition of U , since the difference of the two compositions in question is just $(-\text{ev}_M, \text{id}_M \otimes \delta_{\mathbb{1}^n} \otimes \text{id}_{M^\vee}) \otimes \text{id}_M$. Furthermore the composition of the two vertical arrows on the left is just the identity on M by definition of the dual. Tensoring the big square with U leads to the left square of the next diagram

$$\begin{array}{ccccc}
U \otimes M & \longrightarrow & U \otimes U \otimes \mathbb{1}^n & \xrightarrow{\mu_U \otimes \text{id}_{\mathbb{1}^n}} & U \otimes \mathbb{1}^n \\
\downarrow \text{id} & & \downarrow \text{id}_U \otimes \alpha & & \downarrow \alpha \\
U \otimes M & \xrightarrow{\text{id}_U \otimes u_U \otimes \text{id}_M} & U \otimes U \otimes M & \xrightarrow{\mu_U \otimes \text{id}_M} & U \otimes M
\end{array}$$

where $\alpha := (\mu_U \otimes \text{id}_M) \circ (\text{id} \otimes \delta_M)$. The right square of this diagram also commutes, as is easily checked, and the composition in the bottom row is just the identity according to the constraints on the unit morphism u_U and the multiplication map μ_U . Hence, $\alpha : U \otimes \mathbb{1}^n \rightarrow U \otimes M$ is a split epimorphism in \mathcal{C} , and even in \mathcal{C}_U (since the right square commutes). Since the rank of $v(U \otimes \mathbb{1}^n) = v(U)^n$ and the rank of $v(U \otimes M)$ as $v(U)$ -modules are both n , the split epimorphism $v(\alpha)$ is in fact an isomorphism, i.e. α is an isomorphism.

Applying the natural transformation ε , we finally obtain the commutative square

$$\begin{array}{ccc} U^n = \iota_U((U \otimes \mathbb{1}^n)^{\mathcal{C}}) & \xrightarrow[\cong]{\iota_U(\alpha^{\mathcal{C}})} & \iota_U((U \otimes M)^{\mathcal{C}}) \\ \cong \downarrow \varepsilon_{U^n} & & \downarrow \varepsilon_{M_U} \\ U^n = U \otimes \mathbb{1}^n & \xrightarrow[\cong]{\alpha} & U \otimes M, \end{array}$$

which shows that ε_{M_U} is an isomorphism. Hence, U is a solution ring for M . \square

Remark 5.8. In the case of difference or differential modules over a difference or differential field F , respectively, the ring U constructed in the previous proof is just the usual universal solution algebra $F[X, \det(X)^{-1}]$ for a fundamental solution matrix X having indeterminates as entries. We will therefore call U the **universal solution ring** for M .

This is moreover justified by the following theorem which states that U indeed satisfies a universal property.

Theorem 5.9. *Let R be a solution ring for M , such that $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$ -module, and let U be the solution ring for M constructed in Thm. 5.7. Then there exists a morphism of \mathcal{C} -algebras $f : U \rightarrow R$. Furthermore, the image of $\iota(R^{\mathcal{C}}) \otimes U \xrightarrow{\varepsilon_{R \otimes f}} R \otimes R \xrightarrow{\mu_R} R$ does not depend on the choice of f .*

Proof. By assumption, we have an isomorphism in \mathcal{C}_R :

$$\alpha : R^n \xrightarrow{\cong} \iota_R((M_R)^{\mathcal{C}_R}) = R \otimes_{\iota(R^{\mathcal{C}})} \iota((R \otimes M)^{\mathcal{C}}) \xrightarrow{\cong} R \otimes M.$$

Since M is dualizable, one has bijections

$$\begin{aligned} \text{Mor}_{\mathcal{C}_R}(R^n, R \otimes M) &\simeq \text{Mor}_{\mathcal{C}_R}(R \otimes (\mathbb{1}^n \otimes M^{\vee}), R) && \simeq \text{Mor}_{\mathcal{C}}(\mathbb{1}^n \otimes M^{\vee}, R) \\ \alpha &\mapsto \tilde{\alpha}_R := (\text{id}_R \otimes \text{ev}_M) \circ (\alpha \otimes \text{id}_{M^{\vee}}) && \mapsto \tilde{\alpha} := \tilde{\alpha}_R|_{\mathbb{1}^n \otimes M^{\vee}} \end{aligned}$$

Similarly, for the inverse morphism $\beta := \alpha^{-1} : R \otimes M \rightarrow R^n$, one has

$$\begin{aligned} \text{Mor}_{\mathcal{C}_R}(R \otimes M, R^n) &\simeq \text{Mor}_{\mathcal{C}_R}(R \otimes (M \otimes (\mathbb{1}^n)^{\vee}), R) && \simeq \text{Mor}_{\mathcal{C}}(M \otimes (\mathbb{1}^n)^{\vee}, R) \\ \beta &\mapsto \tilde{\beta}_R := (\text{id}_R \otimes \text{ev}_{\mathbb{1}^n}) \circ (\beta \otimes \text{id}_{(\mathbb{1}^n)^{\vee}}) && \mapsto \tilde{\beta} := \tilde{\beta}_R|_{M \otimes (\mathbb{1}^n)^{\vee}} \end{aligned}$$

Therefore the isomorphism α induces a morphism of \mathcal{C} -algebras

$$f : \text{Sym}\left((M \otimes (\mathbb{1}^n)^{\vee}) \oplus (\mathbb{1}^n \otimes M^{\vee})\right) \rightarrow R.$$

We check that this morphism factors through U , i.e. we have to check that the morphisms

$$M \otimes M^{\vee} \xrightarrow{\text{id} \otimes \delta_{\mathbb{1}^n} \otimes \text{id}} M \otimes (\mathbb{1}^n)^{\vee} \otimes \mathbb{1}^n \otimes M^{\vee} \xrightarrow{\tilde{\beta} \otimes \tilde{\alpha}} R \otimes R \xrightarrow{\mu_R} R$$

and

$$M \otimes M^{\vee} \xrightarrow{\text{ev}_M} \mathbb{1} \xrightarrow{u_R} R$$

are equal. For this we consider the R -linear extensions in the category \mathcal{C}_R . By [7, Sect. 2.4], the composition

$$M_R^{\vee} \xrightarrow{\delta_{R^n} \otimes \text{id}_{M_R^{\vee}}} (R^n)^{\vee} \otimes_R R^n \otimes_R M_R^{\vee} \xrightarrow{\text{id} \otimes \alpha \otimes \text{id}} M_R^{\vee} \otimes_R M_R \otimes_R (R^n)^{\vee} \xrightarrow{\text{id} \otimes \text{ev}_{M_R}} (R^n)^{\vee}$$

is just the transpose ${}^t\alpha : M_R^\vee \rightarrow (R^n)^\vee$ of the morphism α , and this equals the contragredient β^\vee of $\beta = \alpha^{-1}$.

Hence the equality of the two morphisms reduces to the commutativity of the diagram

$$\begin{array}{ccc} M_R \otimes_R M_R^\vee & \xrightarrow{\beta \otimes \beta^\vee} & R^n \otimes_R (R^n)^\vee \\ & \searrow \text{ev}_{M_R} & \downarrow \text{ev}_{R^n} \\ & & R. \end{array}$$

But by definition of the contragredient (see [7, Sect. 2.4]), this diagram commutes.

It remains to show that the image of $\iota(R^C) \otimes U \xrightarrow{\varepsilon_R \otimes f} R \otimes R \xrightarrow{\mu_R} R$ does not depend on the chosen morphism $f : U \rightarrow R$.

Given two morphism of \mathcal{C} -algebras $f, g : U \rightarrow R$, let $\tilde{\alpha}_f, \tilde{\alpha}_g \in \text{Mor}_{\mathcal{C}}(\mathbb{1}^n \otimes M^\vee, R)$ be the restrictions of f resp. of g to $\mathbb{1}^n \otimes M^\vee \subseteq U$, and let $\tilde{\beta}_f, \tilde{\beta}_g \in \text{Mor}_{\mathcal{C}}(M \otimes (\mathbb{1}^n)^\vee, R)$ be the restrictions of f resp. of g to $M \otimes (\mathbb{1}^n)^\vee \subseteq U$. Furthermore, let $\alpha_f, \alpha_g \in \text{Mor}_{\mathcal{C}_R}(R^n, M_R)$ and $\beta_f, \beta_g \in \text{Mor}_{\mathcal{C}_R}(M_R, R^n)$ denote the corresponding isomorphisms. Then by similar considerations as above one obtains that β_f and β_g are the inverses of α_f and α_g , respectively. Then

$$\beta_g \circ \alpha_f \in \text{Mor}_{\mathcal{C}_R}(R^n, R^n) \simeq \text{Hom}_{R^C}((R^C)^n, (R^n)^C) \simeq \text{Mor}_{\mathcal{C}_{\iota(R^C)}}(\iota(R^C)^n, \iota(R^C)^n)$$

is induced by an isomorphism on $\iota(R^C)^n$ (which we also denote by $\beta_g \circ \alpha_f$). Therefore for the $\iota(R^C)$ -linear extension $\tilde{\alpha}_{f, \iota(R^C)}, \tilde{\alpha}_{g, \iota(R^C)} : \iota(R^C) \otimes \mathbb{1}^n \otimes M^\vee \rightarrow R$, one has

$$\begin{aligned} \tilde{\alpha}_{f, \iota(R^C)} &= (\text{id}_R \otimes \text{ev}_M) \circ (\alpha_f|_{\iota(R^C)^n} \otimes \text{id}_{M^\vee}) \\ &= (\text{id}_R \otimes \text{ev}_M) \circ (\alpha_g|_{\iota(R^C)^n} \otimes \text{id}_{M^\vee}) \circ ((\beta_g \circ \alpha_f) \otimes \text{id}_{M^\vee}) \\ &= \tilde{\alpha}_{g, \iota(R^C)} \circ ((\beta_g \circ \alpha_f) \otimes \text{id}_{M^\vee}). \end{aligned}$$

and similarly,

$$\tilde{\beta}_{f, \iota(R^C)} = \tilde{\beta}_{g, \iota(R^C)} \circ ((\alpha_g \circ \beta_f) \otimes \text{id}_{M^\vee}).$$

Hence, the morphism $\mu_R \circ (\varepsilon_R \otimes f) : \iota(R^C) \otimes U \rightarrow R$ factors through $\mu_R \circ (\varepsilon_R \otimes g)$ and by changing the roles of f and g , the morphism $\mu_R \circ (\varepsilon_R \otimes g)$ factors through $\mu_R \circ (\varepsilon_R \otimes f)$. So the images are equal. \square

Remark 5.10. In the classical settings, every Picard-Vessiot ring for some module M is a quotient of the universal solution ring U . This is also the case in this abstract setting (see Thm. 5.12 below). More generally, we will see that every simple minimal solution ring for M (i.e. without the assumption on the constants) is a quotient of U . Conversely, in Cor. 5.16 we show that every quotient of U by a maximal \mathcal{C} -ideal \mathfrak{m} is a Picard-Vessiot ring if $(U/\mathfrak{m})^C = k$. Dropping the assumption $(U/\mathfrak{m})^C = k$, however, one still has a simple solution ring U/\mathfrak{m} (by Prop. 5.5), but U/\mathfrak{m} may not be minimal. To see this, let $M = \mathbb{1}$. Then trivially $R := \mathbb{1}$ is a Picard-Vessiot ring for M , and the only one, since it is contained in any other \mathcal{C} -algebra.

The universal solution ring for $M = \mathbb{1}$, however, is given by $U \cong \mathbb{1} \otimes_k k[x, x^{-1}]$. Hence, for every maximal ideal I of $k[x, x^{-1}]$, $\mathfrak{m} := \iota(I)$ is a maximal \mathcal{C} -ideal of

$U = \iota(k[x, x^{-1}])$ by Lemma 4.3. But $U/\mathfrak{m} \cong \iota(k[x, x^{-1}]/I)$ is only a minimal solution ring, if $k[x, x^{-1}]/I \cong k$, i.e. $U/\mathfrak{m} \cong \mathbb{1}$.

We continue with properties of quotients of U .

Proposition 5.11. *Let U be the universal solution ring for some dualizable $M \in \mathcal{C}$, and let R be a quotient algebra of U . Then $v(R)$ is a finitely generated faithfully flat $\mathcal{O}_{\mathcal{X}}$ -algebra. If in addition R is a simple \mathcal{C} -algebra, then $R^{\mathcal{C}}$ is a finite field extension of k .*

Proof. Since R is a quotient of U , it is a quotient of $T := \text{Sym}\left((M \otimes (\mathbb{1}^n)^{\vee}) \oplus (\mathbb{1}^n \otimes M^{\vee})\right)$. Since $v(M)$ is finitely generated, $v(T)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$ -algebra and therefore also $v(R)$ is a finitely generated $\mathcal{O}_{\mathcal{X}}$ -algebra.

Since M is dualizable, $\langle\langle M \rangle\rangle$ is a Tannakian category (see Rem. 5.2), and T is an ind-object of $\langle\langle M \rangle\rangle$. Being a quotient of T , R also is an ind-object of $\langle\langle M \rangle\rangle$. Therefore by [7, Lemma 6.11], $v(R)$ is faithfully flat over $\mathcal{O}_{\mathcal{X}}$.

If in addition R is simple, $\ell := R^{\mathcal{C}}$ is a field. By exactness of ι and Prop. 3.5(iii), we have a monomorphism $\iota(\ell) \hookrightarrow R$, and hence by exactness of v , an inclusion of $\mathcal{O}_{\mathcal{X}}$ -algebras $\mathcal{O}_{\mathcal{X}} \otimes_k \ell = v(\iota(\ell)) \hookrightarrow v(R)$. After localising to some affine open subset of \mathcal{X} , we can apply Thm. 2.1, and obtain that ℓ is a finite extension of k . \square

Theorem 5.12. *Let M be a dualizable object of \mathcal{C} , and let U be the universal solution ring for M . Then every simple minimal solution ring for M is isomorphic to a quotient of the universal solution algebra U . In particular, every Picard-Vessiot ring for M is isomorphic to a quotient of U .*

Proof. Let R be a simple minimal solution ring for M . Since R is simple, $R^{\mathcal{C}}$ is a field, and therefore $(R \otimes M)^{\mathcal{C}}$ is a free $R^{\mathcal{C}}$ -module. Hence R fulfills the assumptions of Theorem 5.9, and there is a morphism of \mathcal{C} -algebras $f : U \rightarrow R$. As $(U \otimes M)^{\mathcal{C}}$ is a free $U^{\mathcal{C}}$ -module, the image $f(U)$ is a solution ring by Prop. 5.5. As R is minimal, we obtain $f(U) = R$. Hence, R is the quotient of U by the kernel of f . \square

Corollary 5.13. *Let $R \in \mathcal{C}$ be a simple minimal solution ring for some dualizable $M \in \mathcal{C}$. Then $v(R)$ is a finitely generated faithfully flat $\mathcal{O}_{\mathcal{X}}$ -algebra, and $R^{\mathcal{C}}$ is a finite field extension of k .*

Proof. This follows directly from Thm. 5.12 and Prop. 5.11. \square

Proposition 5.14. *Let M be a dualizable object of \mathcal{C} , and let R be a simple solution ring for M with $R^{\mathcal{C}} = k$. Then there is a unique Picard-Vessiot ring for M inside R . This is the image of the universal solution ring U under a morphism $f : U \rightarrow R$.*

Proof. As in the proof of Thm. 5.12, R fulfills the assumptions of Theorem 5.9, so there is a morphism of \mathcal{C} -algebras $f : U \rightarrow R$. By assumption on R , we have $\iota(R^{\mathcal{C}}) = \iota(k) = \mathbb{1}$, and hence $\varepsilon_R \otimes f = f : \mathbb{1} \otimes U = U \rightarrow R$. So by the second part of Theorem 5.9, the image $f(U)$ does not depend on the choice of f . In particular, $f(U)$ (which is a solution ring by Prop. 5.5) is the unique minimal solution ring inside R . It remains to show that $f(U)$ is a simple algebra.

Let $I \subseteq U$ be a maximal subobject in \mathcal{C}_U (i.e. an ideal of U), let $R' := U/I$ and let $g : U \rightarrow R'$ be the canonical epimorphism. Furthermore, let $\mathfrak{m} \in \mathcal{C}$ be a maximal ideal of $R' \otimes R$. Since R and R' are simple, the natural morphisms $R \rightarrow (R' \otimes R)/\mathfrak{m}$ and $R' \rightarrow (R' \otimes R)/\mathfrak{m}$ considered in \mathcal{C}_R and $\mathcal{C}_{R'}$, respectively, are monomorphisms, and it suffices to show that $\mathbb{1} \otimes f(U) \subseteq (R' \otimes R)/\mathfrak{m}$ is simple.

$$\begin{array}{ccc} U & \xrightarrow{f} & R \\ g \downarrow & & \downarrow 1 \otimes \text{id}_R \\ R' & \xrightarrow{\text{id}_{R'} \otimes 1} & (R' \otimes R)/\mathfrak{m} \end{array}$$

$g(U) = R'$ is simple by construction, and so is $g(U) \otimes \mathbb{1} \subseteq (R' \otimes R)/\mathfrak{m}$. By Theorem 5.9, we have $\iota(l) \cdot (g(U) \otimes \mathbb{1}) = \iota(l) \cdot (1 \otimes f(U))$, where $l = ((R' \otimes R)/\mathfrak{m})^{\mathcal{C}}$, and l is a field, since $(R' \otimes R)/\mathfrak{m}$ is simple. By Corollary 4.4, applied to the category $\mathcal{C}_{R'}$, $\iota(l) \cdot (g(U) \otimes \mathbb{1})$ is also simple, i.e. $\iota(l) \cdot (1 \otimes f(U))$ is simple. Since, $\iota(l) \cdot (1 \otimes f(U)) \cong l \otimes_k f(U)$ is a faithfully flat extension of $f(U)$, this implies that $f(U)$ is also simple. \square

Remark 5.15. The previous proposition ensures the existence of Picard-Vessiot rings in special cases. For example, in the differential setting over e.g. $F = \mathbb{C}(t)$, if x is a point which is non-singular for the differential equation, then one knows that the ring of holomorphic functions on a small disc around that point is a solution ring for the equation. Hence, there exists a Picard-Vessiot ring (even unique) for the corresponding differential module inside this ring of holomorphic functions.

Similarly, in the case of rigid analytically trivial pre- t -motives (which form a special case of the difference setting) the field of fractions of a given ring of restricted power series is a simple solution ring for all these modules (cf. [19]).

Corollary 5.16. *Let $M \in \mathcal{C}$ be dualizable, and let \mathfrak{m} be a maximal \mathcal{C} -ideal of the universal solution ring U for M such that $(U/\mathfrak{m})^{\mathcal{C}} = k$. Then U/\mathfrak{m} is a Picard-Vessiot ring for M .*

Proof. By Prop. 5.5, U/\mathfrak{m} fulfills the conditions of R in the previous proposition. Hence, the image of the morphism $U \rightarrow U/\mathfrak{m}$ (which clearly is U/\mathfrak{m}) is a Picard-Vessiot ring. \square

Corollary 5.17. *Let $M \in \mathcal{C}$ be dualizable, and let R and R' be two simple minimal solution rings for M . Then there exists a finite field extension ℓ of k containing $R^{\mathcal{C}}$ and $(R')^{\mathcal{C}}$ such that $R \otimes_{R^{\mathcal{C}}} \ell \cong R' \otimes_{(R')^{\mathcal{C}}} \ell$.*

Proof. As in the proof of the previous theorem, let $f : U \rightarrow R$ and $g : U \rightarrow R'$ be epimorphisms of \mathcal{C} -algebras whose existence is guaranteed by Thm. 5.12. Let \mathfrak{m} be a maximal \mathcal{C} -ideal of $R' \otimes R$, and let $\ell := (R' \otimes R/\mathfrak{m})^{\mathcal{C}}$. Then R' and R embed into $R' \otimes R/\mathfrak{m}$ and hence $(R')^{\mathcal{C}}$ and $R^{\mathcal{C}}$ both embed into ℓ . Furthermore by Thm. 5.9, the subrings $\iota(\ell)(g(U) \otimes 1)$ and $\iota(\ell)(1 \otimes f(U))$ are equal. As ℓ contains both $R^{\mathcal{C}}$ and $(R')^{\mathcal{C}}$, one has $\iota(\ell)(g(U) \otimes 1) = \iota(\ell)(R' \otimes 1) \cong R' \otimes_{(R')^{\mathcal{C}}} \ell$ and $\iota(\ell)(1 \otimes f(U)) \cong R \otimes_{R^{\mathcal{C}}} \ell$. Hence, $R' \otimes_{(R')^{\mathcal{C}}} \ell \cong R \otimes_{R^{\mathcal{C}}} \ell$. As in the proof of Prop. 5.11, one shows that ℓ is indeed finite over k . \square

Theorem 5.18. *Let $M \in \mathcal{C}$ be dualizable. Then there exists a Picard-Vessiot ring for M up to a finite field extension of k , i.e. there exists a finite field extension ℓ of k and a $\mathcal{C}_{\iota(\ell)}$ -algebra R such that R is a PV-ring for $M_{\iota(\ell)} \in \mathcal{C}_{\iota(\ell)}$.*

Proof. Let U be the universal solution ring for M , and let $\mathfrak{m} \subset U$ be a maximal \mathcal{C} -ideal of U . Then $R := U/\mathfrak{m}$ is a simple solution ring for M by Prop. 5.5, and $\ell := R^{\mathcal{C}}$ is a finite field extension of k by Prop. 5.11.

Considering now $M_{\iota(\ell)} \in \mathcal{C}_{\iota(\ell)}$, and R as an algebra in $\mathcal{C}_{\iota(\ell)}$ via $\varepsilon_R : \iota(R^{\mathcal{C}}) = \iota(\ell) \rightarrow R$, we obtain that R is a simple solution ring for $M_{\iota(\ell)}$ with $R^{\mathcal{C}} = \ell$. Hence by Prop. 5.14, with k replaced by ℓ (and \mathcal{C} by $\mathcal{C}_{\iota(\ell)}$ etc.), there is a unique Picard-Vessiot ring for $M_{\iota(\ell)}$ inside R . Indeed also by Prop. 5.14, this Picard-Vessiot ring is R itself, since the canonical morphism $\iota(\ell) \otimes U \rightarrow R$ is an epimorphism, and $\iota(\ell) \otimes U$ is easily seen to be the universal solution ring for $M_{\iota(\ell)}$. \square

6. PICARD-VESSIOT RINGS AND FIBRE FUNCTORS

Throughout this section, we fix a dualizable object $M \in \mathcal{C}$. Recall that we denote by $\langle\langle M \rangle\rangle$ the strictly full tensor subcategory of \mathcal{C} generated by M and M^{\vee} , i.e. the full subcategory of \mathcal{C} containing all objects isomorphic to subquotients of direct sums of objects $M^{\otimes n} \otimes (M^{\vee})^{\otimes m}$ for $n, m \geq 0$.

In this section we consider the correspondence between Picard-Vessiot rings R for M and fibre functors $\omega : \langle\langle M \rangle\rangle \rightarrow \mathbf{vect}_k$. The main result is Thm. 6.5 which states that there is a bijection between their isomorphism classes. This generalises [3, Thm. 3.4.2.3] to our abstract setting.

Proposition 6.1. *Assume R is a Picard-Vessiot ring for M . Then the functor*

$$\omega_R : \langle\langle M \rangle\rangle \rightarrow \mathbf{vect}_k, N \mapsto (R \otimes N)^{\mathcal{C}}$$

is an exact faithful tensor-functor, i.e. a fibre functor.

*We call the fibre functor ω_R the **fibre functor associated to R** .*

Proof. By definition of a Picard-Vessiot ring, the morphism $\varepsilon_{M_R} : R \otimes_k (R \otimes M)^{\mathcal{C}} \rightarrow R \otimes M$ is an isomorphism. Hence, by Prop. 4.8, ε_{N_R} is an isomorphism for all $N \in \langle\langle M \rangle\rangle$.

Recall $R \otimes_k (R \otimes N)^{\mathcal{C}} = \iota_R((N_R)^{\mathcal{C}}) = \iota_R(\omega_R(N))$ for all N .

As $v(R)$ is faithfully flat over $\mathcal{O}_{\mathcal{X}} = v(1)$ by Cor. 5.13, the functor $N \mapsto R \otimes N$ is exact and faithful. Hence, given a short exact sequence $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$ in $\langle\langle M \rangle\rangle$, the sequence

$$0 \rightarrow R \otimes N' \rightarrow R \otimes N \rightarrow R \otimes N'' \rightarrow 0$$

is exact, and $R \otimes N = 0$ if and only if $N = 0$. Using the isomorphisms ε_{N_R} etc. the sequence

$$0 \rightarrow R \otimes_k \omega_R(N') \rightarrow R \otimes_k \omega_R(N) \rightarrow R \otimes_k \omega_R(N'') \rightarrow 0$$

is exact. As ι_R is exact and faithful, this implies that

$$0 \rightarrow \omega_R(N') \rightarrow \omega_R(N) \rightarrow \omega_R(N'') \rightarrow 0$$

is exact. Furthermore, $\omega_R(N) = 0$ if and only if $R \otimes_k \omega_R(N) = 0$ if and only if $R \otimes N = 0$ if and only if $N = 0$.

It remains to show that ω_R is a tensor-functor which is already done by showing that $\varepsilon_{(N \otimes N')_R}$ is an isomorphism if ε_{N_R} and $\varepsilon_{N'_R}$ are. \square

Given a fibre functor $\omega : \langle\langle M \rangle\rangle \rightarrow \mathbf{vect}_k$, we want to obtain a Picard-Vessiot ring associated to ω .

Apparently, this Picard-Vessiot ring is already given in the proof of [8, Thm. 3.2], although the authors don't claim that it is a Picard-Vessiot ring. We will recall the construction to be able to prove the necessary facts:

For $N \in \langle\langle M \rangle\rangle$, one defines P_N to be the largest subobject of $N \otimes_k \omega(N)^\vee$ such that for all $n \geq 1$ and all subobjects $N' \subseteq N^n$, the morphism

$$P_N \rightarrow N \otimes_k \omega(N)^\vee \xrightarrow{\text{diag}} N^n \otimes_k \omega(N^n)^\vee \rightarrow N^n \otimes_k \omega(N')^\vee$$

factors through $N' \otimes_k \omega(N')^\vee$.

For monomorphisms $g : N' \rightarrow N$ and epimorphisms $g : N \rightarrow N'$, one obtains morphisms $\phi_g : P_N \rightarrow P_{N'}$, and therefore

$$R_\omega := \varinjlim_{N \in \langle\langle M \rangle\rangle} P_N^\vee \in \text{Ind}(\langle\langle M \rangle\rangle) \subseteq \mathcal{C}$$

is welldefined. The multiplication $\mu_{R_\omega} : R_\omega \otimes R_\omega \rightarrow R_\omega$ is induced by the natural morphisms $P_{N \otimes L} \rightarrow P_N \otimes P_L$ via dualizing and taking inductive limits.

Lemma 6.2. *The functor $\mathcal{C}\text{-Alg} \rightarrow \mathbf{Sets}$ which associates to each \mathcal{C} -algebra R' the set of natural tensor-transformations from the functor $R' \otimes (\iota \circ \omega) : \langle\langle M \rangle\rangle \rightarrow \mathcal{C}_{R'}$ to the functor $R' \otimes \text{id}_{\langle\langle M \rangle\rangle} : \langle\langle M \rangle\rangle \rightarrow \mathcal{C}_{R'}$ is represented by the \mathcal{C} -algebra R_ω , i.e. there is a natural bijection between the natural transformations $R' \otimes (\iota \circ \omega) \rightarrow R' \otimes \text{id}_{\langle\langle M \rangle\rangle}$ of tensor functors and the morphisms of \mathcal{C} -algebras $R_\omega \rightarrow R'$.*

Proof. Let R' be a \mathcal{C} -algebra, and let α be a natural transformation not necessarily respecting the tensor structure. Then for every $N \in \langle\langle M \rangle\rangle$ one has a morphism

$$\begin{aligned} \alpha_N &\in \text{Mor}_{\mathcal{C}_{R'}}(R' \otimes \iota(\omega(N)), R' \otimes N) \simeq \text{Mor}_{\mathcal{C}}(\iota(\omega(N)), R' \otimes N) \\ &\simeq \text{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes N \otimes \iota(\omega(N))^\vee) = (R' \otimes N \otimes \iota(\omega(N))^\vee)^{\mathcal{C}} \end{aligned}$$

It is straight forward to check that such a collection of morphisms $(\alpha_N)_N$ where $\alpha_N \in \text{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes N \otimes \iota(\omega(N))^\vee)$ defines a natural transformation if and only if $\alpha_N \in \text{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes P_N)$ for all N , and $\alpha_{N'} = (\text{id}_{R'} \otimes \phi_g) \circ \alpha_N$ whenever $\phi_g : P_N \rightarrow P_{N'}$ is defined.

On the other hand, one has

$$\begin{aligned} \text{Mor}_{\mathcal{C}}(R_\omega, R') &= \text{Mor}_{\mathcal{C}}(\varinjlim_{N \in \langle\langle M \rangle\rangle} P_N^\vee, R') \\ &= \varprojlim_{N \in \langle\langle M \rangle\rangle} \text{Mor}_{\mathcal{C}}(P_N^\vee, R') \simeq \varprojlim_{N \in \langle\langle M \rangle\rangle} \text{Mor}_{\mathcal{C}}(\mathbb{1}, R' \otimes P_N) \end{aligned}$$

Hence, giving such a compatible collection of morphisms α_N is equivalent to giving a \mathcal{C} -morphism $R_\omega \rightarrow R'$.

It is also not hard to check that the natural transformations that respect the tensor structure correspond to morphisms of \mathcal{C} -algebras $R \rightarrow R'$ under this identification. \square

Before we show that R_ω is a simple solution ring for M , we need some more results from [8] resp. from [7]:

As ω has values in k -vector spaces, $\langle\langle M \rangle\rangle$ together with ω is a neutral Tannakian category (see [7]), and therefore equivalent to the category of representations of the algebraic group scheme $G = \underline{\text{Aut}}^\otimes(\omega)$.

This also induces an equivalence of their ind-categories, and R_ω corresponds to the group ring $k[G]$ with the right regular representation (cf. proof of [8, Theorem 3.2]).

Proposition 6.3. *The object $R_\omega \in \text{Ind}(\langle\langle M \rangle\rangle) \subseteq \mathcal{C}$ associated to ω is a simple solution ring for M , and satisfies $(R_\omega)^\mathcal{C} = k$.*

Remark 6.4. By Prop. 5.14, R_ω therefore contains a unique Picard-Vessiot ring for M . This Picard-Vessiot ring will be called the **PV-ring associated to ω** . Indeed, R_ω is already minimal and hence a Picard-Vessiot ring itself. This will be seen at the end of the proof of Thm. 6.5. There is also a way of directly showing that R_ω is isomorphic to a quotient of the universal solution ring for M which would also imply that R_ω is a PV-ring (cf. Cor. 5.16). But we don't need this here, so we will omit it.

Proof. As ω defines an equivalence of categories $\langle\langle M \rangle\rangle \rightarrow \text{Rep}_k(G)$ (and also of their ind-categories), and $\omega(R_\omega) = k[G]$, one obtains

$$(R_\omega)^\mathcal{C} = \text{Mor}_\mathcal{C}(\mathbf{1}, R_\omega) \simeq \text{Hom}_G(k, k[G]) = k[G]^G = k.$$

For showing that R_ω is simple, let $I \neq R_\omega$ be an ideal of R_ω in \mathcal{C} . We even have $I \in \text{Ind}(\langle\langle M \rangle\rangle)$, as it is a subobject of R . By the equivalence of categories $\omega(I)$ belongs to $\text{Ind}(\text{Rep}_k(G))$, and $\omega(I)$ is an ideal of $\omega(R_\omega) = k[G]$. But $k[G]$ does not have non-trivial G -stable ideals. Hence, $\omega(I) = 0$, and therefore $I = 0$.

As seen in Lemma 6.2, $\text{id}_{R_\omega} \in \text{Mor}_\mathcal{C}(R_\omega, R_\omega)$ induces a natural transformation $\alpha : R_\omega \otimes (\iota \circ \omega) \rightarrow R_\omega \otimes \text{id}_{\langle\langle M \rangle\rangle}$, in particular it induces a \mathcal{C}_{R_ω} -morphism $\alpha_M : R_\omega \otimes \iota(\omega(M)) \rightarrow R_\omega \otimes M$. By [8, Prop. 1.13], such a natural transformation is an equivalence, as $\langle\langle M \rangle\rangle$ is rigid⁵. Therefore, the morphism α_M is an isomorphism. As $R_\omega \otimes \iota(\omega(M)) = \iota_{R_\omega}(\omega(M))$, Lemma 4.7 implies that ε_{M_R} is an isomorphism. Hence, R_ω is a solution ring for M . □

Theorem 6.5. *Let $M \in \mathcal{C}$ be dualizable, and let ℓ be a field extension of k . Then there is a bijection between isomorphism classes of Picard-Vessiot rings R for $M_{\iota(\ell)}$ over $\tilde{\mathbf{1}} := \iota(\ell)$ and isomorphism classes of fibre functors ω from $\langle\langle M_{\iota(\ell)} \rangle\rangle$ into ℓ -vector spaces.*

This bijection is induced by $R \mapsto \omega_R$ and $\omega \mapsto (\text{PV-ring inside } R_\omega)$ given in Prop. 6.1 and Rem. 6.4, respectively.

Proof. Clearly isomorphic Picard-Vessiot rings give rise to isomorphic fibre functors and isomorphic fibre functors give rise to isomorphic Picard-Vessiot rings. Hence, we only have to show that the maps are inverse to each other up

⁵Rigidity of the target category which is assumed in loc. cit. is not needed. See also [5, Prop. 1.1].

to isomorphisms.

By working directly in the category $\mathcal{C}_{\iota(\ell)}$ we can assume that $\ell = k$.

On one hand, for given ω and corresponding PV-ring R , one has natural isomorphisms

$$\iota_R(\omega(N)) = R \otimes_k \omega(N) \rightarrow N_R$$

(see proof of Prop. 6.3). By adjunction these correspond to natural isomorphisms

$$\lambda_N : \omega(N) \cong (N_R)^{\mathcal{C}} = \omega_R(N),$$

i.e. the functors ω and ω_R are isomorphic.

Conversely, given a Picard-Vessiot ring R and associated fibre functor ω_R , let R_ω be the simple solution ring constructed above.

As $\iota_R = R \otimes \iota$ and $(N_R)^{\mathcal{C}_R} = \omega_R(N)$ for all $N \in \langle\langle M \rangle\rangle$, the natural isomorphisms $\varepsilon_{N_R} : \iota_R((N_R)^{\mathcal{C}_R}) \rightarrow N_R$ form a natural transformation $R \otimes (\iota \circ \omega_R) \rightarrow R \otimes \text{id}_{\langle\langle M \rangle\rangle}$. By Lemma 6.2, this natural transformation corresponds to a morphism of \mathcal{C} -algebras $\varphi : R_\omega \rightarrow R$. As R_ω is a simple \mathcal{C} -algebra, φ is a monomorphism. But R is a minimal solution ring, and hence φ is even an isomorphism. Therefore, R_ω is isomorphic to R and already minimal, i.e. R_ω is a Picard-Vessiot ring itself. \square

7. GALOIS GROUP SCHEMES

Given a dualizable object $M \in \mathcal{C}$ and a Picard-Vessiot ring R for M , one considers the group functor

$$\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R) : \text{Alg}_k \rightarrow \text{Groups}$$

which associates to each k -algebra D the group of automorphisms of $R \otimes_k D$ as an algebra in $\mathcal{C}_{\iota(D)}$, i.e. the subset of $\text{Mor}_{\mathcal{C}_{\iota(D)}}(R \otimes_k D, R \otimes_k D)$ consisting of all isomorphisms which are compatible with the algebra structure of $R \otimes_k D$.

This functor is called the **Galois group of R over 1** .

On the other hand, given a fibre functor $\omega : \langle\langle M \rangle\rangle \rightarrow \text{vect}_k$, one considers the group functor

$$\underline{\text{Aut}}^{\otimes}(\omega) : \text{Alg}_k \rightarrow \text{Groups}$$

which associates to each k -algebra D the group of natural automorphisms of the functor $D \otimes_k \omega : N \mapsto D \otimes_k \omega(N)$.

As $\langle\langle M \rangle\rangle$ together with the fibre functor ω is a neutral Tannakian category, this group functor is called the **Tannakian Galois group** of $(\langle\langle M \rangle\rangle, \omega)$. In [7] it is shown that this group functor is indeed an algebraic group scheme.

The aim of this section is to show that both group functors are isomorphic algebraic group schemes if $\omega = \omega_R$ is the fibre functor associated to R .

We start by recalling facts about group functors, (commutative) Hopf-algebras and affine group schemes. All of this can be found in [25].

A group functor $\text{Alg}_k \rightarrow \text{Groups}$ is an affine group scheme over k if it is representable by a commutative algebra over k . This commutative algebra then has a structure of a Hopf-algebra. The group functor is even an algebraic group scheme (i.e. of finite type over k) if the corresponding Hopf-algebra is finitely generated.

The category of commutative Hopf-algebras over k and the category of affine

group schemes over k are equivalent. This equivalence is given by taking the spectrum of a Hopf-algebra in one direction and by taking the ring of regular functions in the other direction.

For a Hopf-algebra H over k , and corresponding affine group scheme $\mathcal{G} := \text{Spec}(H)$, the category $\text{Comod}(H)$ of right comodules of H and the category $\text{Rep}(\mathcal{G})$ of representations of \mathcal{G} are equivalent. This equivalence is given by attaching to a comodule V with comodule map $\rho : V \rightarrow V \otimes_k H$ the following representation $\varrho : \mathcal{G} \rightarrow \text{End}(V)$ of \mathcal{G} : For any k -algebra D and $g \in \mathcal{G}(D) = \text{Hom}_{k\text{-alg}}(H, D)$, the endomorphism $\varrho(g)$ on $V \otimes_k D$ is the D -linear extension of

$$g \circ \rho : V \rightarrow V \otimes_k H \rightarrow V \otimes_k D.$$

On the other hand, for any representation $\varrho : \mathcal{G} \rightarrow \text{End}(V)$, the universal element $\text{id}_H \in \text{Hom}_{k\text{-alg}}(H, H) = \mathcal{G}(H)$ gives a H -linear homomorphism $\varrho(\text{id}_H) : V \otimes_k H \rightarrow V \otimes_k H$, and its restriction to $V \otimes 1$ is the desired comodule map $\rho : V \rightarrow V \otimes_k H$.

For showing that the group functors $\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R)$ and $\underline{\text{Aut}}^{\otimes}(\omega_R)$ are isomorphic algebraic group schemes, we show that they are both represented by the k -vector space $H := (R \otimes R)^{\mathcal{C}} = \omega_R(R)$. The next lemma shows that H is a finitely generated (commutative) k -Hopf-algebra, and hence $\text{Spec}(H)$ is an algebraic group scheme over k .

Remark 7.1. This fact is shown for differential modules over algebraically closed constants in [24, Thm. 2.33], and for t-motives in [19, Sections 3.5-4.5].

Lemma 7.2. *Let R be a PV-ring for M and $H := \omega_R(R) = (R \otimes R)^{\mathcal{C}}$.*

- (i) *The morphism $\varepsilon_{RR} : R \otimes_k H \rightarrow R_R = R \otimes R$ is an isomorphism in \mathcal{C}_R (with R -module structure on $R \otimes R$ given on the first factor).*
- (ii) *H is a finitely generated commutative k -algebra where the structure maps $u_H : k \rightarrow H$ (unit), $\mu_H : H \otimes_k H \rightarrow H$ (multiplication) are given by*

$$u_H := \omega_R(u_R) \quad \text{and} \quad \mu_H := \omega_R(\mu_R),$$

respectively.

- (iii) *The k -algebra H is even a Hopf-algebra where the structure maps $c_H : H \rightarrow k$ (counit), $\Delta : H \rightarrow H \otimes_k H$ (comultiplication) and $s : H \rightarrow H$ (antipode) are given as follows: Counit and antipode are given by*

$$c_H := (\mu_R)^{\mathcal{C}} \quad \text{and} \quad s := (\tau)^{\mathcal{C}},$$

respectively, where $\tau \in \text{Mor}_{\mathcal{C}}(R \otimes R, R \otimes R)$ denotes the twist morphism. The comultiplication is given by

$$\Delta := \omega_R(\varepsilon_{RR}^{-1} \circ (u_R \otimes \text{id}_R)) \quad ^6$$

Remark 7.3. The definition of Δ might look strange. Compared to other definitions (e.g. in [22, Sect. 2]), where Δ is the map on constants/invariants induced by the map $R \otimes R \rightarrow R \otimes R \otimes R, a \otimes b \mapsto a \otimes 1 \otimes b$, one might think that Δ should be defined as $(\text{id}_R \otimes u_R \otimes \text{id}_R)^{\mathcal{C}} = \omega_R(u_R \otimes \text{id}_R)$. The reason for the

⁶Hence, Δ is the image under ω_R of the morphism $R \xrightarrow{u_R \otimes \text{id}_R} R \otimes R \xrightarrow{\varepsilon_{RR}^{-1}} R \otimes_k H$

difference is that in [22] and others, one uses $(R \otimes R) \otimes_R (R \otimes R) \cong R \otimes R \otimes R$ with right- R -module structure on the left tensor factor $(R \otimes R)$ and left- R -module structure on the right tensor factor $(R \otimes R)$.

In our setting, however, we are always using left- R -modules. In particular, the natural isomorphism $\omega_R(R) \otimes_k \omega_R(R) \rightarrow \omega_R(R \otimes R)$ reads as

$$\text{Mor}_{\mathcal{C}_R}(R, R \otimes R) \otimes_k \text{Mor}_{\mathcal{C}_R}(R, R \otimes R) \rightarrow \text{Mor}_{\mathcal{C}_R}(R, R \otimes R \otimes R)$$

where the left hand side is isomorphic to $\text{Mor}_{\mathcal{C}_R}(R, (R \otimes R) \otimes_R (R \otimes R))$. But here, this is the tensor product of left- R -modules.

The additional ε_{RR}^{-1} in the definition of Δ solves the problem. It is also implicitly present in the identification $H \otimes_k H \cong (R \otimes R \otimes R)^{\mathcal{C}}$ in [22] (cf. proof of Lemma 2.4(b) loc. cit.).

Proof of Lemma 7.2. As R is an object of $\text{Ind}(\langle\langle M \rangle\rangle)$, part (i) follows from Prop. 4.8. As ω_R is a tensor functor, it is clear that the structure of a commutative algebra of R induces a structure of a commutative algebra on $\omega_R(R) = H$ via the maps u_H and μ_H defined in the lemma. As in the proof of Prop. 5.11, one verifies that $H = \omega_R(R)$ is finitely generated as k -algebra.

Part (iii) is obtained by checking that the necessary diagrams commute. We only show that Δ is coassociative, i.e. that $(\Delta \otimes_k \text{id}_H) \circ \Delta = (\text{id}_H \otimes_k \Delta) \circ \Delta$, and leave the rest to the reader.

As $\Delta = \omega_R(\varepsilon_{RR}^{-1} \circ (u_R \otimes \text{id}_R))$, $\Delta \otimes_k \text{id}_H = \omega_R((\varepsilon_{RR}^{-1} \otimes_k \text{id}_H) \circ (u_R \otimes \text{id}_R \otimes_k \text{id}_H))$ and $\text{id}_H \otimes_k \Delta = \omega_R(\text{id}_R \otimes_k \Delta)$, it suffices to show that the morphisms

$$(\varepsilon_{RR}^{-1} \otimes_k \text{id}_H) \circ (u_R \otimes \text{id}_R \otimes_k \text{id}_H) \circ \varepsilon_{RR}^{-1} \circ (u_R \otimes \text{id}_R) \quad \text{and}$$

$$(\text{id}_R \otimes_k \Delta) \circ \varepsilon_{RR}^{-1} \circ (u_R \otimes \text{id}_R)$$

are equal. This is seen by showing that the following diagram commutes:

$$\begin{array}{ccccc} R & \xrightarrow{u_R \otimes \text{id}_R} & R \otimes R & \xrightarrow{\varepsilon_{RR}^{-1}} & R \otimes_k H \\ \downarrow u_R \otimes \text{id}_R & & \downarrow u_R \otimes \text{id}_{R \otimes R} & & \downarrow u_R \otimes \text{id}_{R \otimes_k H} \\ R \otimes R & \xrightarrow{\text{id}_R \otimes u_R \otimes \text{id}_R} & R \otimes R \otimes R & \xrightarrow{\text{id}_R \otimes \varepsilon_{RR}^{-1}} & R \otimes R \otimes_k H \\ \downarrow \varepsilon_{RR}^{-1} & & & & \downarrow \varepsilon_{RR}^{-1} \otimes_k \text{id}_H \\ R \otimes_k H & \xrightarrow{\text{id}_R \otimes_k \Delta = \iota_R(\Delta)} & & & R \otimes_k H \otimes_k H \end{array}$$

Obviously the upper squares commute. Let $\delta := \varepsilon_{RR}^{-1} \circ (u_R \otimes \text{id}_R)$. Then the middle horizontal morphism equals $\text{id}_R \otimes \delta$ and the lower horizontal morphism is $\iota_R(\Delta) = \iota_R((\text{id}_R \otimes \delta)^{\mathcal{C}_R})$. As ε is a natural transformation $\iota_R \circ ()^{\mathcal{C}_R} \rightarrow \text{id}_{\mathcal{C}_R}$, and as $\varepsilon_{RR}^{-1} \otimes_k \text{id}_H = \varepsilon_{(R \otimes_k H)_R}^{-1}$, also the lower square commutes. \square

Theorem 7.4. *Let R be a PV-ring for M . Then the group functor*

$$\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R) : \text{Alg}_k \rightarrow \text{Groups}$$

is represented by the Hopf-algebra $H = \omega_R(R) = (R \otimes R)^{\mathcal{C}}$. Furthermore $\text{Spec}(v(R))$ is a torsor of $\underline{\text{Aut}}_{\mathcal{C}\text{-alg}}(R)$ over X .

Proof. This is shown similar to [16, Prop.10.9] or [10]. One has to use that

$$\delta : R \xrightarrow{u_R \otimes \text{id}_R} R \otimes R \xrightarrow{\varepsilon_{RR}^{-1}} R \otimes_k H$$

defines a right coaction of H on R . The property of a right coaction, however, is given by the commutativity of the diagram in the proof of Lemma 7.2. The torsor property is obtained by the isomorphism $v(\varepsilon_{RR}^{-1}) : v(R) \otimes_{\mathcal{O}_X} v(R) \rightarrow v(R) \otimes_k H$. \square

Theorem 7.5. *Let R be a PV-ring for M and $H = \omega_R(R)$.*

(i) *For all $N \in \langle\langle M \rangle\rangle$, $\rho_N : \omega_R(N) \rightarrow H \otimes_k \omega_R(N)$ given by*

$$\rho_N := \omega_R(\varepsilon_{NR}^{-1} \circ (u_R \otimes \text{id}_N)) \quad ^7$$

defines a left coaction of H on $\omega_R(N)$.

(ii) *The collection $\rho := (\rho_N)_{N \in \langle\langle M \rangle\rangle}$ is a natural transformation of tensor functors $\omega_R \mapsto H \otimes_k \omega_R$, where $H \otimes_k \omega_R$ is a functor $\langle\langle M \rangle\rangle \rightarrow \mathbf{Mod}_H$.*

Remark 7.6. By going to the inductive limit one also gets a map $\rho_R : \omega_R(R) \rightarrow H \otimes_k \omega_R(R)$. This map is nothing else then the comultiplication $\Delta : H \rightarrow H \otimes_k H$.

Proof of Thm. 7.5. Part (i) is proven in the same manner as the coassociativity of Δ . For proving the second part, recall that ε is a natural transformation. Hence, for every morphism $f : N \rightarrow N'$ the diagram

$$\begin{array}{ccccc} N & \xrightarrow{u_R \otimes \text{id}_N} & R \otimes N & \xrightarrow{\varepsilon_{NR}^{-1}} & R \otimes_k \omega_R(N) \\ f \downarrow & & \text{id}_R \otimes f \downarrow & & \downarrow \iota_R((\text{id}_R \otimes f)^c) \\ N' & \xrightarrow{u_R \otimes \text{id}_{N'}} & R \otimes N' & \xrightarrow{\varepsilon_{N'R}^{-1}} & R \otimes_k \omega_R(N') \end{array}$$

commutes. As $\iota_R((\text{id}_R \otimes f)^c) = \text{id}_R \otimes_k \omega_R(f)$, applying ω_R to the diagram gives the desired commutative diagram for ρ being a natural transformation. Compatibility with the tensor product is seen in a similar way. \square

Theorem 7.7. *Let R be a PV-ring for M and $H = \omega_R(R)$. Then the group functor*

$$\underline{\text{Aut}}^\otimes(\omega_R) : \text{Alg}_k \rightarrow \text{Groups}$$

*is represented by the Hopf-algebra H .*⁸

Proof. As $\rho := (\rho_N)_{N \in \langle\langle M \rangle\rangle}$ defines a left coaction of H on the functor ω_R by natural transformations, one obtains a right action of $\text{Spec}(H)$ on ω_R . Composing with the antipode (i.e. taking inverse group elements), one therefore gets a homomorphism of group functors

$$\varphi : \text{Spec}(H) \rightarrow \underline{\text{Aut}}^\otimes(\omega_R).$$

⁷The map $\varepsilon_{NR}^{-1} \circ (u_R \otimes \text{id}_N)$ is a morphism in \mathcal{C} : $N \rightarrow R \otimes N \rightarrow R \otimes_k \omega_R(N)$

⁸As shown in the following proof, the representing Hopf-algebra naturally is the coopposite Hopf-algebra H^{cop} of H . However, the antipode s is an isomorphism of Hopf-algebras $s : H \rightarrow H^{\text{cop}}$, hence $H^{\text{cop}} \cong H$.

Explicitly, for any k -algebra D and $h \in H(D) = \text{Hom}_{k\text{-alg}}(H, D)$, one defines $\varphi(h) \in \underline{\text{Aut}}^\otimes(\omega_R)(D) = \text{Aut}^\otimes(D \otimes_k \omega_R)$ as the natural transformation which for $N \in \langle\langle M \rangle\rangle$ is the D -linear extension of the composition

$$\omega_R(N) \xrightarrow{\rho_N} H \otimes_k \omega_R(N) \xrightarrow{s \otimes \text{id}_{\omega_R(N)}} H \otimes_k \omega_R(N) \xrightarrow{h \otimes \text{id}_{\omega_R(N)}} D \otimes_k \omega_R(N).$$

For showing that the homomorphism φ is indeed an isomorphism, we give the inverse map:

For any k -algebra D and $g \in \underline{\text{Aut}}^\otimes(\omega_R)(D)$, one has the homomorphism $g_R \in \text{End}_D(D \otimes_k \omega_R(R)) = \text{End}_D(D \otimes_k H)$, and one defines $\psi(g) \in H(D)$ as the composition

$$H \xrightarrow{s} H \xrightarrow{u_D \otimes \text{id}_H} D \otimes_k H \xrightarrow{g_R} D \otimes_k H \xrightarrow{\text{id}_D \otimes c_H} D.$$

It is a straight forward calculation to check that $\psi(g)$ is indeed a homomorphism of k -algebras and that φ and ψ are inverse to each other. \square

Corollary 7.8. *The affine group schemes $\underline{\text{Aut}}_{\mathcal{C}\text{-Alg}}(R)$ and $\underline{\text{Aut}}^\otimes(\omega_R)$ are isomorphic.*

Proof. By Thm. 7.4 and Thm. 7.7 both functors are represented by the Hopf-algebra $H = \omega_R(R)$. \square

8. GALOIS CORRESPONDENCE

In this section we will establish a Galois correspondence between subalgebras of a PV-ring and closed subgroups of the corresponding Galois group. As in [18], the Galois correspondence will only take into account subalgebras which are PV-rings themselves on the one hand, and normal subgroups on the other.

We start by recalling facts about sub-Hopf-algebras and closed subgroup schemes which can be found in [25].

In the equivalence of affine group schemes and Hopf-algebras, closed subgroup schemes correspond to Hopf-ideals, and closed normal subgroup schemes correspond to so called normal Hopf-ideals. As there is a correspondence between closed normal subgroup schemes and factor group schemes of \mathcal{G} by taking the cokernel and the kernel, respectively, there is also a correspondence between normal Hopf-ideals and sub-Hopf-algebras ([21, Thm. 4.3]). This correspondence is given by

$$I \mapsto H(I) := \text{Ker} \left(H \xrightarrow{\Delta - \text{id}_H \otimes u_H} H \otimes_k H \rightarrow H \otimes_k (H/I) \right),$$

for a normal Hopf-ideal I , and by

$$H' \mapsto (H')^+ H,$$

for a sub-Hopf-algebra H' , where $(H')^+$ is defined to be the kernel of the counit $c_{H'} : H' \rightarrow k$.

Furthermore, for a sub-Hopf-algebra $H' \subseteq H$, the category $\text{Comod}(H')$ embeds into $\text{Comod}(H)$ as a full subcategory.

Theorem 8.1. *Let $M \in \mathcal{C}$ be dualizable, R a PV-ring for M (assuming it exists), $\omega = \omega_R$ the corresponding fibre functor, $H = \omega_R(R)$, and $\mathcal{G} = \text{Spec}(H) = \underline{\text{Aut}}_{\mathcal{C}\text{-Alg}}(R) = \underline{\text{Aut}}^{\otimes}(\omega)$ the corresponding Galois group. Then there is a bijection between*

$$\mathfrak{T} := \{T \in \mathcal{C}\text{-Alg} \mid T \subseteq R \text{ is PV-ring for some } N \in \langle\langle M \rangle\rangle\}$$

and

$$\mathfrak{N} := \{\mathcal{N} \mid \mathcal{N} \leq \mathcal{G} \text{ closed normal subgroup scheme of } \mathcal{G}\}$$

given by $\Psi : \mathfrak{T} \rightarrow \mathfrak{N}, T \mapsto \underline{\text{Aut}}_{\mathcal{C}_T\text{-Alg}}(R)$ resp. $\Phi : \mathfrak{N} \rightarrow \mathfrak{T}, \mathcal{N} \mapsto R^{\mathcal{N}}$.

Here, the ring of invariants $R^{\mathcal{N}}$ is the largest subobject T of R such that for all k -algebras D and all $\sigma \in \mathcal{N}(D) \subset \text{Aut}_{\mathcal{C}_{\iota(D)}}(R \otimes_k D)$, one has $\sigma|_{T \otimes_k D} = \text{id}_{T \otimes_k D}$. Equivalently, $R^{\mathcal{N}}$ is the equalizer of the morphisms $\text{id}_R \otimes u_{k[\mathcal{N}]} : R \rightarrow R \otimes_k k[\mathcal{N}]$ ⁹ and $R \xrightarrow{\delta} R \otimes_k H \twoheadrightarrow R \otimes_k k[\mathcal{N}]$, where $\delta = \varepsilon_{R_R}^{-1} \circ (u_R \otimes \text{id}_R)$ is the comodule map of R as H -comodule, and $H \twoheadrightarrow k[\mathcal{N}]$ is the canonical epimorphism.

Proof of Thm. 8.1. The functor ω_R is an equivalence of categories

$$\omega_R : \langle\langle M \rangle\rangle \rightarrow \text{comod}(H),$$

and also of their ind-categories.¹⁰ Hence, it provides a bijection between subalgebras of R in \mathcal{C} and subalgebras of H stable under the left comodule structure. We will show that under this bijection sub-PV-rings correspond to sub-Hopf-algebras and that this bijection can also be described as given in the theorem. First, let $T \subseteq R$ be a PV-ring for some $N \in \langle\langle M \rangle\rangle$. Then $\langle\langle N \rangle\rangle$ is a full subcategory of $\langle\langle M \rangle\rangle$, and the fibre functor $\omega_T : \langle\langle N \rangle\rangle \rightarrow \text{vect}_k$ corresponding to T is nothing else than the restriction of ω_R to the subcategory $\langle\langle N \rangle\rangle$, as T is a subobject of R . Hence, $H' := \omega_R(T) = \omega_T(T)$ is a sub-Hopf-algebra of H . Therefore, we obtain a closed normal subgroup scheme of $\mathcal{G} = \text{Spec}(H)$ as the kernel of $\text{Spec}(H) \twoheadrightarrow \text{Spec}(H')$. As $\text{Spec}(H) = \underline{\text{Aut}}_{\mathcal{C}\text{-Alg}}(R)$ and $\text{Spec}(H') = \underline{\text{Aut}}_{\mathcal{C}\text{-Alg}}(T)$, this kernel is exactly $\underline{\text{Aut}}_{\mathcal{C}_T\text{-Alg}}(R)$.

On the other hand, let \mathcal{N} be a closed normal subgroup scheme of $\mathcal{G} = \text{Spec}(H)$ defined by a normal Hopf-ideal I of H , and

$$H' = \text{Ker} \left(H \xrightarrow{\Delta - \text{id}_H \otimes u_H} H \otimes_k H \twoheadrightarrow H \otimes_k (H/I) \right)$$

the corresponding sub-Hopf-algebra of H .

The subcategory $\text{comod}(H')$ is generated by one object V (as every category of finite comodules is), and the object $N \in \langle\langle M \rangle\rangle$ corresponding to V via ω_R , has a PV-ring T inside R by Thm. 5.18, since R is a simple solution ring for N with $R^{\mathcal{C}} = k$. Furthermore, since T is the PV-ring corresponding to the fibre functor $\omega_R : \langle\langle N \rangle\rangle \rightarrow \text{comod}(H')$, we have $\omega_R(T) = H'$.

It remains to show that $T = R^{\mathcal{N}}$, i.e. that

$$T = \text{Ker} \left(R \xrightarrow{\delta - \text{id}_R \otimes u_H} R \otimes_k H \twoheadrightarrow R \otimes_k k[\mathcal{N}] = R \otimes_k (H/I) \right).$$

⁹ $k[\mathcal{N}] := \mathcal{O}_{\mathcal{N}}(\mathcal{N})$ denotes the ring of regular functions on the affine scheme \mathcal{N} .

¹⁰Here, $\text{comod}(H)$ denotes the category of left- H -comodules which are finite-dimensional as k -vector spaces.

As ω_R is an equivalence of categories, this is equivalent to

$$\omega_R(T) = \text{Ker} \left(\omega_R(R) \xrightarrow{\omega_R(\delta) - \omega_R(\text{id}_R) \otimes_k u_H} \omega_R(R) \otimes_k H \twoheadrightarrow \omega_R(R) \otimes_k (H/I) \right).$$

But, as $\omega_R(T) = H'$, $\omega_R(R) = H$ and $\omega_R(\delta) = \Delta$, this is just the definition of H' . \square

REFERENCES

- [1] Katsutoshi Amano. *Relative invariants, difference equations, and the Picard-Vessiot theory*. PhD thesis, University of Tsukuba, Tsukuba, Japan, 2005.
- [2] Katsutoshi Amano and Akira Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *J. Algebra*, 285(2):743–767, 2005.
- [3] Yves André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Ann. Sci. École Norm. Sup. (4)*, 34(5):685–739, 2001.
- [4] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.
- [5] Alain Bruguières. Théorie tannakienne non commutative. *Comm. Algebra*, 22(14):5817–5860, 1994.
- [6] Phyllis J. Cassidy and Michael F. Singer. Galois theory of parameterized differential equations and linear differential algebraic groups. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 113–155. Eur. Math. Soc., Zürich, 2007.
- [7] P. Deligne. Catégories tannakiennes. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 111–195. Birkhäuser Boston, Boston, MA, 1990.
- [8] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih. Tannakian Categories. In *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*, pages 101–228. Springer-Verlag, Berlin, 1982.
- [9] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.
- [10] Tobias Dyckerhoff. The inverse problem of differential Galois theory over the field $\mathbb{R}(z)$. Preprint, 2008.
- [11] Charlotte Hardouin and Michael F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [12] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.
- [13] Saunders Mac Lane. Categorical algebra. *Bull. Amer. Math. Soc.*, 71:40–106, 1965.
- [14] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.
- [15] B. Heinrich Matzat and Marius van der Put. Iterative differential equations and the Abhyankar conjecture. *J. Reine Angew. Math.*, 557:1–52, 2003.
- [16] Andreas Maurischat. Galois theory for iterative connections and nonreduced Galois groups. *Trans. Amer. Math. Soc.*, 362(10):5411–5453, 2010.
- [17] Andreas Maurischat. Infinitesimal group schemes as iterative differential Galois groups. *J. Pure Appl. Algebra*, 214(11):2092–2100, 2010.
- [18] Andreas Maurischat. Picard-Vessiot theory of differentially simple rings. *J. Algebra*, 409:162–181, 2014.
- [19] Matthew A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Invent. Math.*, 171(1):123–174, 2008.
- [20] Émile Picard. *Traité d’analyse. Tome III*. Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1991. Des singularités des équations différentielles. Étude du cas où la variable reste réelle. Des courbes définies par des équations différentielles. Équations linéaires; analogies entre les équations

algébriques et les équations linéaires. Intégration de certaines équations aux dérivées partielles avec des conditions aux limites, [Singularities of differential equations. Study of the case in which the variable remains real. Curves defined by differential equations. Linear equations; analogies between algebraic equations and linear equations. Integration of some partial differential equations with boundary conditions], Reprint of the third (1928) edition.

- [21] Mitsuhiro Takeuchi. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.*, 7:251–270, 1972.
- [22] Mitsuhiro Takeuchi. A Hopf algebraic approach to the Picard-Vessiot theory. *J. Algebra*, 122(2):481–509, 1989.
- [23] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
- [24] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.
- [25] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.
- [26] Michael Wibmer. *Geometric Difference Galois Theory*. PhD thesis, Heidelberg University, Heidelberg, Germany, 2010.

Andreas Maurischat, Lehrstuhl A für Mathematik, RWTH Aachen University, Germany
E-mail address: andreas.maurischat@matha.rwth-aachen.de